管理者ガイド

Dr.Web® Anti-virus for Linux
バージョン <%PRODUCTVERSION%>
User Manual
23.01.2012

ロシア本社
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125124

ウェブサイト www.drweb.com
電話 +7 (495) 789-45-87

地方支店、オフィスに関する情報は、弊社のオフィシャルサイトにあります。

Doctor Web

弊社はマルウェアおよび迷惑メールに対する効率的な保護を
提供する Dr.WebR 情報セキュリティソリューションの
開発および販売を行っています。

個人ユーザから政府機関、また中小企業から国際的な企業まで、
世界中のあらゆる地域に弊社のお客様は広がっています。

Dr.Web アンチウイルスソリューションは 1992年以来、
卓越したマルウェアの検出能力と国際的な情報
セキュリティ基準への適合で良く知られています。
Dr.Web ソリューションには政府による認証や表彰が
何度も与えられていること、また弊社製品のユーザが
世界中に広がっていることは、弊社製品に対する
皆さまからの絶大な信頼の証しだと自負しています。

弊社の全てのお客さまからの多大なるご支援と
ご貢献に心より感謝いたします。

目次

表記規則

本書では、以下の文字・記号を使用しています。

文字・記号	意味
太字	グラフィカルインターフェース（GUI）の要素の名称や本書のとおり正確に入力する必要のある入力例
緑色の太字	**Doctor Web** 製品またはコンポーネントの名称
緑色で下線付きの文字	本書の他のページや他のWebページへのリンク
`固定幅フォント`	コマンドラインの入力例、出力例
イタリック体	ユーザが提供しなければならない情報を表すプレースホルダ。コマンドラインの入力例がイタリック体の場合は、パラメータ値を示します。
大太字	キーボードのキー名称
プラス記号 ('+')	キーの同時押し（例：ALT+F1 は、ALTキーとF1キーを同時に押すことを意味します。）
感嘆符	重要な注釈、またはエラーなどを引き起こす可能性のある状況に関する警告

チャプター1. はじめに

Dr.Web® Anti-virus for Linux をご購入いただき有難うございます。本製品は最先端のウイルス検出・駆除テクノロジーにより、様々なタイプのコンピュータ脅威からの信頼できる保護を提供します。

本マニュアルには、GNU/Linuxコンピュータへの **Dr.Web Anti-virus for Linux** バージョン6.0.2のインストールおよび使用方法を記載しています。

Dr.Web Anti-virus for Linuxについて

Dr.Web Anti-virus for Linux は、ウイルスやその他の脅威からGNU/Linuxコンピュータを保護するためのアンチウイルスソリューションです。

プログラムのコアコンポーネント（*アンチウイルスエンジン*および*ウイルスデータベース*）は、非常に効率的かつ省リソースなだけでなく、クロスプラットフォームでもあります。それにより、**Doctor Web** のスペシャリスト達による異なるOSに対する優れたアンチウイルスソリューションの作成が可能となります。 **Dr.Web Anti-virus for Linux** のコンポーネントは常時アップデートされ、最先端の保護を確実なものにするため、ウイルスデータベースには新しい署名が追加されています。また、ヒューリスティック解析を用いて未知のウイルスからも保護します。

Dr.Web Anti-virus for Linux は、それぞれ独自の機能で動作する以下のコンポーネントで構成されています。

コンポーネント	説明
スキャナ	このウイルス検出コンポーネントは以下の目的で使用されます。 • ユーザの要求に応じた、またはスケジュールに沿ったクイック、フル、カスタムスキャン。 • 検出された脅威の駆除（修復、削除、隔離）。アクションは脅威のタイプごとに、ユーザによって手動で、または **Dr.Web Anti-virus for Linux** の設定に応じて自動で選択されます。
SpIDer Guard	リアルタイムで全てのファイル（使用中の）を検査する、常駐するアンチウイルスコンポーネントです。
隔離	感染したファイルやその他の脅威がシステムに害を与えないよう、それらを隔離する為の特別なフォルダです。
アップデータ	ユーザの要求に応じて、またはスケジュールに沿ってウイルスデータベースやその他のプログラムコンポーネントをアップデートするための自動アップデートユーティリティです。
ライセンスマネージャ	キーファイルの管理を簡易化します。デモキーファイルおよびライセンスキーファイルの受け取り、それらに関する情報の閲覧、お持ちのライセンスの更新を可能にします。
スケジューラ	システムの検査、およびプログラムのアップデートをスケジュールに沿って実行する際に必要なコンポーネントです。**Dr.Web Anti-virus for Linux** を停止しても スケジューラ はアクティブなままです。

Dr.Web Anti-virus for Linux の柔軟な設定によって、様々なイベントに対する通知音、隔離 の最大サイズ、検査から除外するファイルおよびフォルダのリストなどを調整することが出来ます。

チャプター2. インストールとアンインストール

このチャプターでは、UNIXシステムでの **Dr.Web Anti-virus for Linux** のインストールおよびアンインストールの手順を説明します。操作の実行にはroot権限が必要です。

既にインストールされている古いバージョンの全てのパッケージ（rpmまたはdebフォーマットで提供された）を、慎重にアンインストールしてください。

Dr.Web Anti-virus for Linux のディストリビューションパッケージは、ESPパッケージマネージャ（EPM）との使用が可能なEPMフォーマット（インストールおよびアンインストールスクリプト、標準インストール／アンインストールGUIを持った）で提供しています。これらのスクリプトは全て、**Dr.Web Anti-virus for Linux** のコンポーネントではなくEPMパッケージ自体のものです。

Dr.Web Anti-virus for Linux のインストールとアンインストール、及びアップグレードは以下の方法で行うことが出来ます。

- インストール／アンインストールGUI経由で
- インストール／アンインストール用コンソールスクリプト経由で

インストールの際には依存関係が判断されます。例えば、あるコンポーネントをインストールする場合、他のコンポーネントがいくつかインストールされている必要があり（例えば、`drweb-daemon`パッケージをインストールするには`drweb-common`および`drweb-bases`がインストールされている必要があります）、それらは自動的にインストールされます。

EPMパッケージからの他の **Dr.Web** 製品がいくつかインストールされているコンピューターに **Dr.Web Anti-virus for Linux** をインストールする場合、アンインストールGUI経由でモジュールを削除しようとする度に、他の製品のものを含む全ての **Dr.Web** モジュールを削除するように要求されます。

必要なコンポーネントを誤って削除してしまわないよう、アンインストールの際に実行する動作と選択は慎重に行うようにしてください。

システム要件

Dr.Web Anti-virus for Linux は、以下の要件を満たすシステムで使用することができます。

コンポーネント	要件
CPU	32bit/64bitモードでのx86プロセッサのコマンドと互換性があります。64bit環境では32bitアプリケーションの動作をサポートする必要があります。
ハードディスクの空き	少なくとも154 MBの空きディスク、および各ユーザごとに70 MB。隔離 内にあるオブジェクトの量およびサイズによってはそれ以上の空き容量が必要な場合があります。
OS	カーネル 2.6.x.のGNU/Linux。
その他	**Dr.Web** ウイルスデータベース および **Dr.Web Anti-virus for Linux** コンポーネントのアップデートにはインターネット接続が必要です。

グラフィカルインターフェース(GUI)によるインストールを行うには、この他にX Window Systemの環境が必要です。X Window Systemが利用できない場合は、インストール用スクリプトを使用してインストールを行います。

また、以下のライブラリとユーティリティがインストールされている必要があります。

- `libglade2`
- `libgtk2`
- `base64`
- `unzip`
- `crond`

対応するLinux製品

Dr.Web Anti-virus for Linux ソリューションは、x86 および x86 64ビットの Linux 製品と互換性があります。

総合的な操作性は、下記のディストリビューションでテストされています。

- ALT Linux バージョン 4 - 6 (32ビット)、バージョン 5-6 (64ビット)
- Arch Linux (64ビット)
- ASPLinux バージョン 12 - 14 (32ビット)
- Debian バージョン 3.1 - 6 (32ビット)、バージョン 4-6 (64ビット)
- Fedora 14 (64-bit)ビット
- Gentoo
- Mandriva Linux バージョン 2009、 CS4 (32ビット)、 2010.x (64ビット)
- Mandrake 10
- openSUSE バージョン 10.3-11 (32/64ビット)
- PCLinuxOS 2010
- Red Hat Enterprise Linux (RHEL) バージョン 4 - 6 (32ビット)、バージョン 5 - 6 (64ビット)
- Suse Linux Enterprise Server バージョン 9 - 11 (32ビット)、バージョン 10-11 (64ビット)
- Ubuntu バージョン 7.04 - 11.04

要件を満たす他のディストリビューションもサポートされていますが、テストはされていません。もしお使いのLinux ディストリビューションで互換性に問題が確認された場合は、http://support.drweb.com/request/からテクニカルサポートにお問い合わせください。

パッケージファイルロケーション

Dr.Web Anti-virus for Linux ソリューションはデフォルトで/opt/drweb/, /etc/drweb/, /var/drweb/ディレクトリおよび~/.drweb/ディレクトリにインストールされます。これらのディレクトリ内にOSに依存しないディレクトリツリーが作成されます。

- /opt/drweb/ - 実行可能モジュール、およびアップデートモジュール **Dr.Web Updater** (Perlスクリプト update.pl)。
- /opt/drweb/lib/ - **Dr.Web Anti-virus for Linux** パッケージの様々なサービスライブラリ。
- /opt/drweb/lib/jp_scanner.dwl - **Dr.Web Scanner** パッケージの言語ファイル。
- /opt/drweb/doc/ - ユーザ設定ファイルおよびドキュメンテーションのプロトタイプ。全てのドキュメンテーションは英語及びロシア語のプレーンテキストファイル(KOI8-R 、UTF-8 エンコード)になっています。
- /opt/drweb/man/ - ソフトウェアコンポーネントのMANファイル。
- /opt/drweb/epm/ - 実行ファイル、言語ファイル、およびグラフィカルアンインストーラのライブラリ。
- /etc/drweb/ - ソフトウェアの様々なコンポーネントのオリジナル設定ファイル: drweb32.ini, drweb-spider.conf
- /etc/drweb/drweb-spider/templates/ - メッセージ内で悪意のあるオブジェクトを検出した時や、**Daemon** またはプラグインの動作中にエラーが発生した後に、異なる種類の受信者に送信する通知のテンプレートです。
- /var/drweb/bases/*.vdb - 既に知られているウイルスのデータベースです。
- /var/drweb/lib/ - ローダブルライブラリとしてのアンチウイルスエンジン(drweb32.dll)。
- ~/.drweb/ - アンチウイルスエンジン、ユーザ設定ファイル、ライセンスキーファイル、プロセスおよびログファイルのPIDファイル。
- ~/.drweb/quarantine/ - 感染したファイルを移すユーザ隔離(そのようなアクションが指定されている場合)。
- ~/.drweb/bases/*.vdb - ユーザホームディレクトリ内にある既に知られたウイルスのデータベース。

64bit環境では/opt/drweb/内にlib64サブディレクトリが作成され、
64bitモジュールの動作に必要なライブラリが含まれています。

Dr.Web for Linuxのインストール

Dr.Web Anti-virus for Linux は、自己抽出パッケージとして提供されます。

drweb-workstations_[version number]~linux_x86.run (32-bit環境)

または drweb-workstations_[version number]~linux_amd64.run (64-bit環境)

パッケージには、以下のコンポーネントが含まれています。

- drweb-common: 設定ファイル(drweb32.ini)、ライブラリ、ドキュメント、ディレクトリ構造。インストールの際に、drwebユーザとdrwebグループが作成されます。
- drweb-bases: ウイルス検査エンジン、ウイルス定義ファイル。drweb-commonパッケージがインストールされている必要があります。
- drweb-updater: ウイルス検査エンジンとウイルス定義ファイルのアップデートユーティリティ。drweb-common、drweb-libsパッケージがインストールされている必要があります。
- drweb-daemon: **Dr.Web Daemon** の実行ファイル、ドキュメント。drweb-bases、drweb-libsパッケージがインストールされている必要があります。
- drweb-scanner: **Dr.Web Scanner** の実行ファイル、ドキュメント。drweb-bases、drweb-libsパッケージがインストールされている必要があります。
- drweb-libs: すべてのコンポーネントに必要な共通ライブラリ
- drweb-epm6.0.2-libs: GUI インストーラ・アンインストーラ のライブラリ。drweb-libsパッケージがインストールされている必要があります。
- drweb-epm6.0.2-uninst: GUIアンインストーラ に必要なファイル。drweb-epm6.0.2-libsパッケージがインストールされている必要があります。
- drweb-cc: **Dr.Web Control Center** 実行ファイル、ドキュメント。drweb-spider、drweb-scanner、および drweb-updaterパッケージがインストールされている必要があります。

- drweb-boost147: **Dr.Web Control Center** と **Dr.Web Spider** の共通ライブラリ。drweb-libsパッケージがインストールされている必要があります。
- drweb-agent: contains **Dr.Web Control Agent** の実行ファイル、ドキュメント。drweb-boost147、drweb-common パッケージがインストールされている必要があります。
- drweb-agent-es: contains files required to run集中管理モードで、**Dr.Web Agent** を動作させるために必要なファイル、ドキュメント。drweb-agent、drweb-updater、drweb-scanner がインストールされている必要があります。
- drweb-monitor: **Dr.Web Monitor** の実行ファイル、ドキュメント。 drweb-common、drweb-boost147パッケージがインストールされている必要があります。
- drweb-spider: **Dr.Web Spider** の実行ファイル、ドキュメント。drweb-daemon、drweb-boost147パッケージがインストールされている必要があります。

64bit版のパッケージにはdrweb-libs および drweb-libs32も含まれています。それぞれ64-bitコンポーネントおよび32-bitコンポーネントのライブラリが含まれています。

Dr.Web Anti-virus for Linux のすべてのコンポーネントを自動的にインストールするためにコンソール(CLI)または、GUIベースのシェルを使用することができます。前者の場合、以下のようなコマンドでインストールパッケージに実行権を与えてください。

```
# chmod +x drweb-workstations_[version number]~linux_x86.run
```

GUI インストーラによるインストール

1. GUIインストーラを

```
# drweb-workstations_[version number]~linux_x86/install.sh
```

のコマンドで実行すると、プログラムセットアップウィンドウが表示されます。

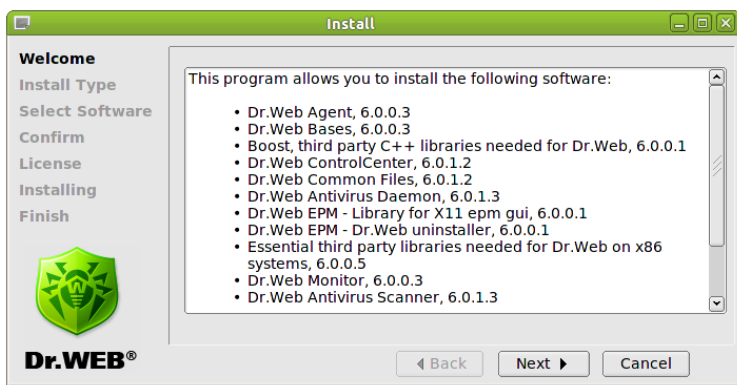



図 1. 起動画面

2. 現在のバージョンではインストールの種別は1つのみで、デフォルトで全てのコンポーネントが選択された **Dr.Web Anti-virus for Linux** の通常の設定になります。

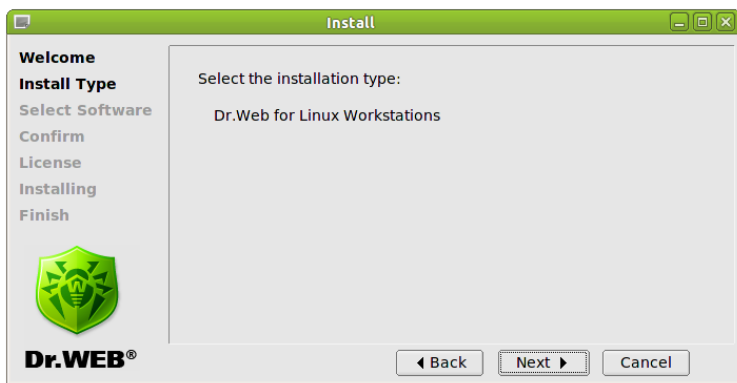



図 2. インストール種別画面

3. **Confirm** 画面で選択を確認してください。

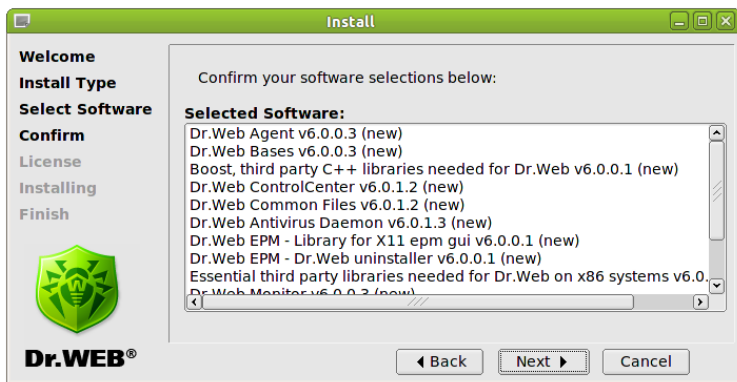



図 3. 確認画面

4. ソフトウェア使用許諾契約が表示されます。インストールを続けるには同意してください。必要に応じ、**Language** リストで言語を選択してください。

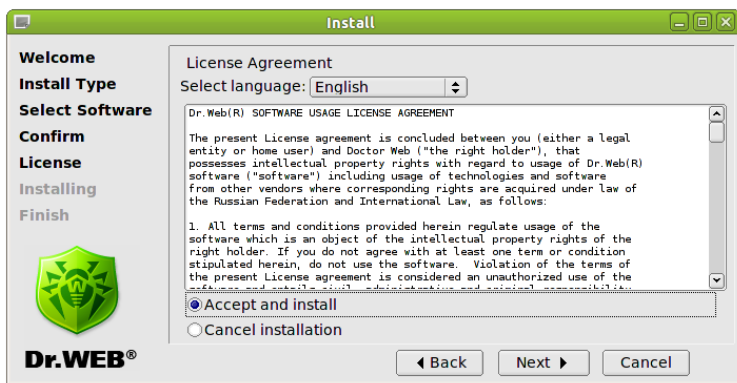



図 4. ソフトウェア使用許諾契約

1. **Installing** 画面でインストールのプロセスをリアルタイムで確認することが出来ます。

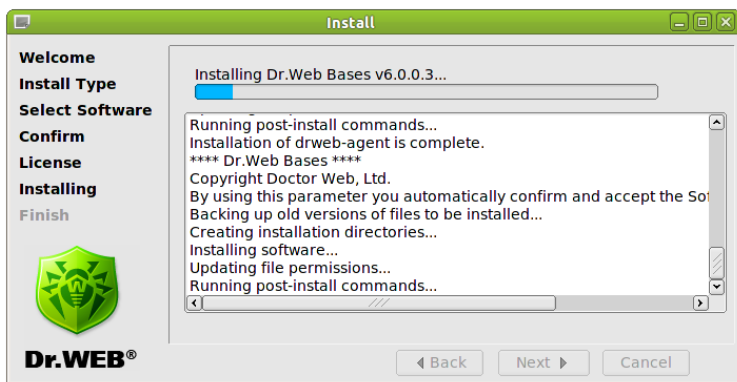



図 5. Installing画面

同時に、インストール処理のログが`drweb-workstations_[version number]~linux_x86`ディレクトリの`install.log`ファイルに記録されます。

5. **Finish** 画面で、インストール処理の結果に関する情報を確認します（成功または失敗）。

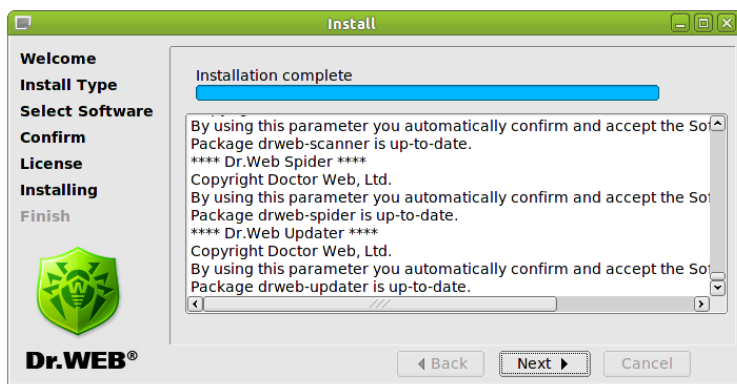
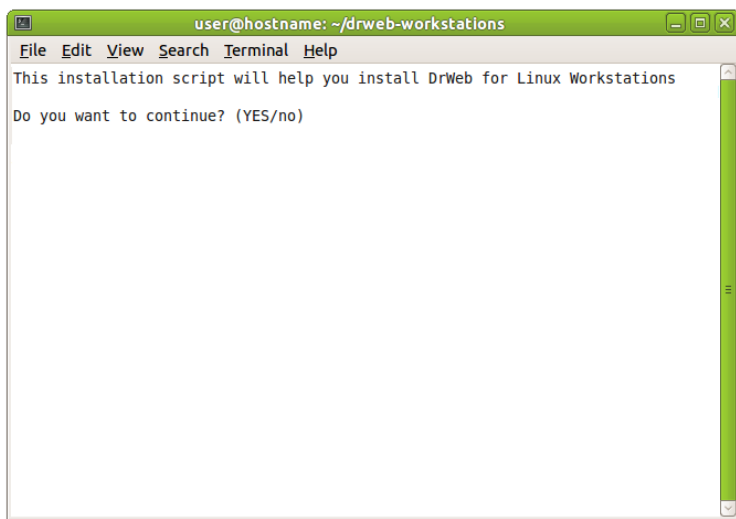
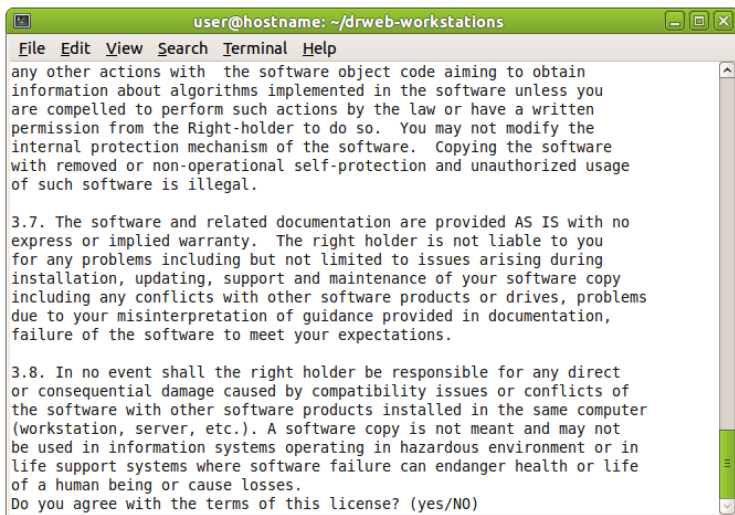
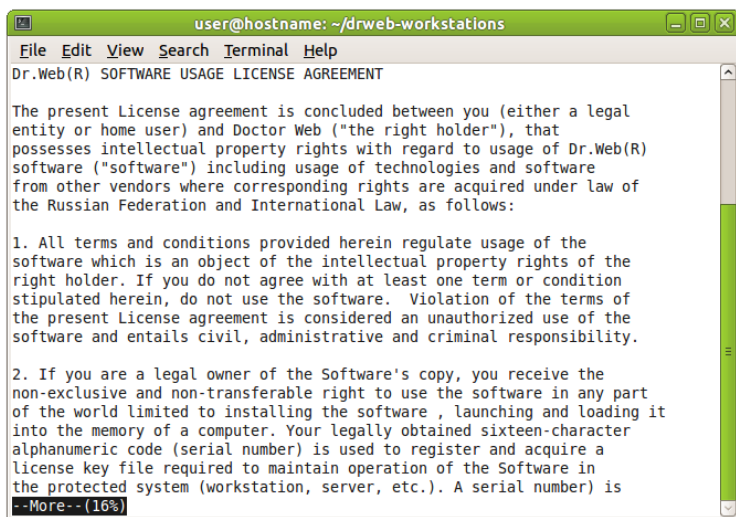



図 6. 終了画面

6. **"Close"** をクリックしてセットアップを終了します。

コンソールインストーラによるインストール

GUIインストールが行えない場合、自動的にコンソールインストーラが開始されます。

コンソールインストーラが起動すると、対話式ウィンドウが表示されます。

Dr.Web Anti-virus for Linux をインストールする場合、**Y** または **Yes** を入力します。インストールしない場合は、 **N** または **No** を入力します（大文字と小文字は区別しません）。 入力後、ENTERキーを押してください。

ソフトウェア使用許諾が表示されます。スペースキーでソフトウェア使用許諾のページを進めることができます。

インストールを続けるにはソフトウェア使用許諾に同意し、**Y** または **Yes** を入力してください。インストールが開始されます。

すぐにインストールが開始されます。コンソールでインストールのプロセスをリアルタイムで確認することが出来ます。

コンソールインストーラが自動で起動しなかった場合（例えば、必要な権限が無い場合など）、root権限によって以下のコマンドを手動で起動してください。

```
# drweb-workstations_[version number]~linux_x86/setup.sh
```

Dr.Web for Linuxのアンインストール

GUIアンインストーラ 経由で **Dr.Web Anti-virus for Linux** の全てのコンポーネントを削除するには、以下のコマンドを実行します。

```
# /opt/drweb/remove.sh
```

root権限がない場合は、rootのパスワードを要求されます。

GUIアンインストーラが起動しない場合は、インタラクティブコンソールアンインストーラ が起動します。

アンインストール後、drwebユーザとdrwebグループをシステムから削除することができます。

アンインストールによって以下の処理が行われます。

- オリジナルの設定ファイルを　/etc/drweb/software/conf/ ディレクトリから削除します。
- ユーザによって設定ファイルのコピーが変更されていなかった場合、それらも削除されます。もし変更が行われていた場合は、保持します。
- **Dr.Web**　のその他のファイルが削除されます。インストール時に古いファイルのコピーが作成されていた場合（通常[file_name].O　という名前）、インストール前の名前で復元されます。
- ライセンスキーファイルとログファイルはそれぞれ対応するディレクトリに残されます。
- ~/.drweb ディレクトリの中身は保持されます。（手動で削除することが出来ます）。

スケジュールに沿って動作させる為に、ユーザcronを使用します。**Dr.Web Anti-virus for Linux** のスタートアップおよび登録後、ユーザの crontab に アップデータ の周期に関する以下のようなエントリがあります。

```
*/30 * * * * sh -c "(/home/user/.drweb/crontab-check.sh /opt/drweb/scripts/drweb-cc/update.sh 2>&1)>>/home/user/.drweb/crontab-updater.log"
```

スキャナ のスケジュールは **Dr.Web Anti-virus for Linux** の **Settings**

セクション内で 対応する機能が有効にされた 後にのみ crontab にエントリされます。

```
0 9 * * * sh -c "(DISPLAY=:0.0 /home/user/.drweb/crontab-check.sh /opt/drweb/scripts/drweb-cc/start-scanning.sh 2>&1)>>/home/user/.drweb/crontab-scan.log"
```

Dr.Web Anti-virus for Linux をアンインストールしても、ユーザ crontab 内の対応するエントリは自動では削除されません。手動で削除する必要があります。

GUIアンインストーラによるアンインストール

1. **Applications** -> **Dr.Web** -> **Removal of Dr.Web for Linux** メニューを使用して、または以下のコマンドでコンソールからGUIを起動すると、

```
# /opt/drweb/remove.sh
```

セットアッププログラムが起動します。

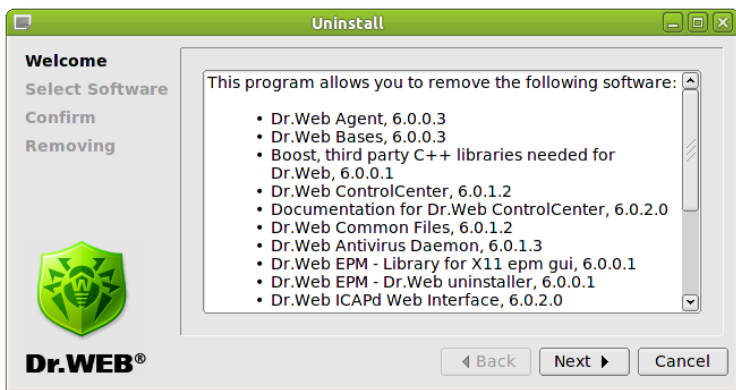



図 7. 起動画面

"Next" をクリックして次に進みます。インストールを終了する場合は、**"Cancel"** をクリックします。

2. **Select Software** 画面で、削除するコンポーネントを選択します。依存関係のあるコンポーネントは自動的に選択されます。

   Dr.Web Anti-virus for Linux がインストールされているコンピューターに、EPM-packagesによって他の **Dr.Web** 製品がインストールされている場合、GUI経由でモジュールを削除しようとする度に、他の製品のものを含む全ての **Dr.Web** モジュールを削除するように要求されます。必要なコンポーネントを誤って削除してしまわないよう、アンインストールの際に実行する動作とコンポーネントの選択は慎重に行うようにしてください。

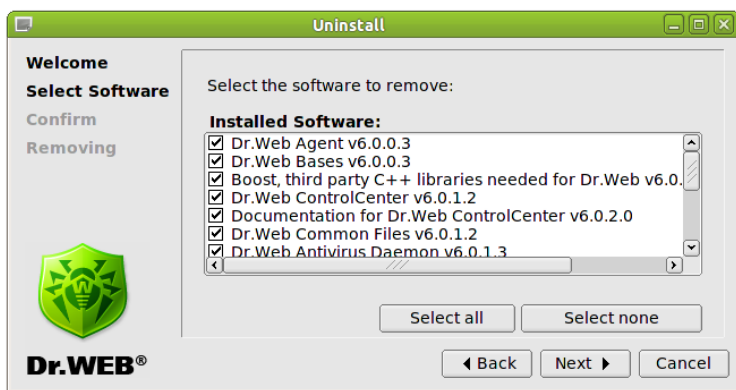



図 8. Select Software画面

"Select All" をクリックすると、全てのコンポーネントが選択され、**"Select None"** をクリックすると、全ての選択が解除されます。

3. **Confirm** 画面でアンインストールするコンポーネントを確認してください。

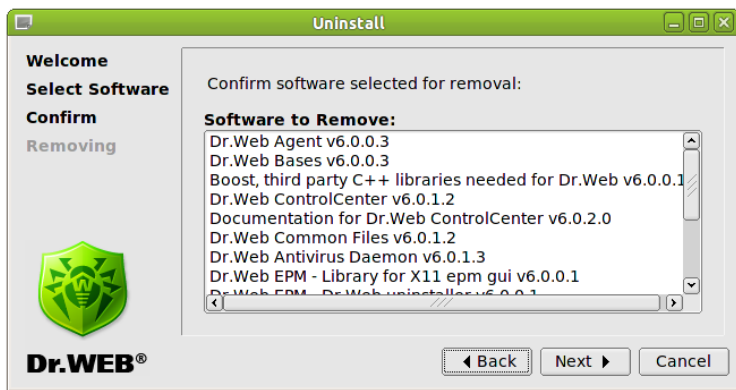



図 9. Confirm画面

4. **Removing** 画面でアンインストールのプロセスをリアルタイムで確認することが出来ます。

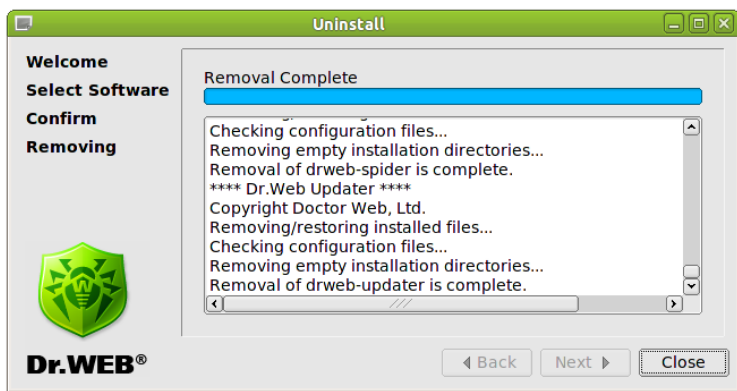
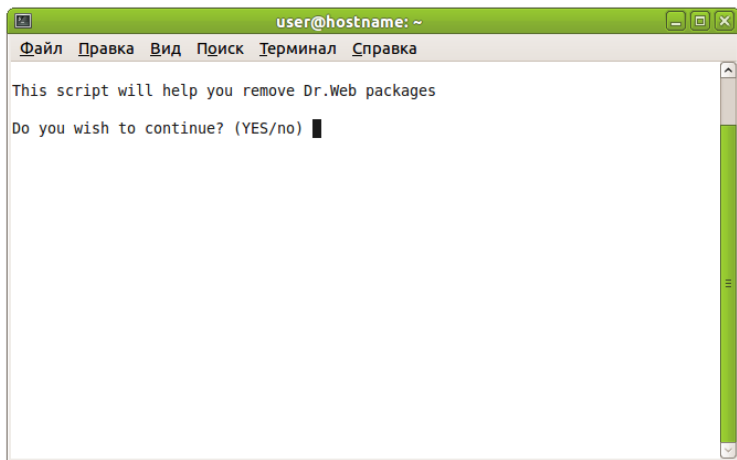



図 10. Removing画面

5. **"Close"**をクリックしてセットアップを終了します。

コンソールアンインストーラによるアンインストール

GUIアンインストールを行えない場合、自動的にコンソールアンインストーラが開始します。

1. コンソールアンインストーラが起動すると、対話式ウィンドウが表示されます。

スクリーンの指示に従って、アンインストールするコンポーネントを選択します。

選択が終了したら、**Y** または **Yes** を入力してENTERキーを押してください（大文字と小文字は区別しません）。

アンインストールログがリアルタイムでコンソールに出力されます。

ネイティブパッケージからのインストール

全てのパッケージは**Dr.Web** の公式リポジトリ http://officeshield.drweb.com/drweb/ に置かれています。お使いのシステムのパッケージマネージャにこのリポジトリを追加すると、リポジトリからのその他のプログラム同様、必要なパッケージをインストール・アップデート・アンインストール出来るようになります。依存関係は自動的に解決されます。

リポジトリを追加、キーをインポート、パッケージをインストール・アンインストールするための以下のコマンドは全て、管理者(root)権限で実行してください。

Debian、Ubuntu (apt)

Debianリポジトリはライセンスキーによってデジタル署名されています。正常に動作する為に、キーを以下のコマンドでインポートする必要があります。

```
wget -O - http://officeshield.drweb.com/drweb/drweb.key | apt-key add -
```

または

```
curl http://officeshield.drweb.com/drweb/drweb.key | apt-key add -
```

お使いのシステムにリポジトリを追加するには `/etc/apt/sources.list` ファイルに以下のラインを追加してください。

```
deb http://officeshield.drweb.com/drweb/debian stable non-free
```

Dr.Web Anti-virus for Linux をインストールするには以下のコマンドを使用します。

```
apt-get update
```

```
apt-get install drweb-cc
```

Dr.Web Anti-virus for Linux をアンインストールするには以下のコマンドを使用します。

```
apt-get remove drweb-cc
```

またはグラフィカルマネージャ(Synapticなど)を使ってパッケージをインストール、アンインストールすることも出来ます。

ALT Linux、PCLinuxOS (apt-rpm)

お使いのシステムにリポジトリを追加するには /etc/apt/sources.list ファイルに以下のラインを追加してください。

32-bit version:

```
rpm http://officeshield.drweb.com/drweb/altlinux stable/i386
drweb
```

64-bit version:

```
rpm http://officeshield.drweb.com/drweb/altlinux stable/x86_64
drweb
```

Dr.Web Anti-virus for Linux をインストールするには以下のコマンドを使用します。

```
apt-get update
```

```
apt-get install drweb-cc
```

Dr.Web Anti-virus for Linux をアンインストールするには以下のコマンドを使います。

```
apt-get remove drweb-cc
```

またはグラフィカルマネージャ(Synapticなど)を使ってパッケージをインストール、アンインストールすることも出来ます。

Mandriva (urpmi)

http://officeshield.drweb.com/drweb/drweb.key からリポジトリキーをダウンロードし、ディスクに保存します。次に、キーを以下のコマンドでインポートしてください。

```
rpm --import <path to repository key>
```

以下のファイルを開いてください。

http://officeshield.drweb.com/drweb/drweb-i386.urpmi-media

または

http://officeshield.drweb.com/drweb/drweb-x86_64.urpmi-media

ファイルを開くと、リポジトリをシステムに加えるように促されます。

または、コンソールを使用して以下のコマンドでリポジトリを追加することも出来ます。

```
urpmi.addmedia drweb http://officeshield.drweb.com/drweb/mandriva/stable/
i386/
```

または

```
urpmi.addmedia drweb http://officeshield.drweb.com/drweb/
mandriva/stable/x86_64/
```

Dr.Web Anti-virus for Linux をインストールするには以下のコマンドを使用します。

```
urpmi.update drweb

urpmi drweb-cc
```

Dr.Web Anti-virus for Linux をアンインストールするには以下のコマンドを使用します。

```
urpme drweb-cc
```

またはグラフィカルマネージャ(rpmdrakeなど)を使ってパッケージをインストール、アンインストールすることも出来ます。

Red Hat Enterprise Linux、Fedora、CentOS (yum)

以下のコンテンツのファイルを `/etc/yum.repos.d` ディレクトリに追加してください。

32-bit version:

```
[drweb]

name=DrWeb - stable
```

```
baseurl=http://officeshield.drweb.com/drweb/el5/stable/i386/
gpgcheck=1
enabled=1
gpgkey=http://officeshield.drweb.com/drweb/drweb.key
```

64-bit version:

```
[drweb]

name=DrWeb - stable
baseurl=http://officeshield.drweb.com/drweb/el5/stable/x86_64/
gpgcheck=1
enabled=1
gpgkey=http://officeshield.drweb.com/drweb/drweb.key
```

Dr.Web Anti-virus for Linux をインストールするには以下のコマンドを使用します。

```
yum install drweb-cc
```

Dr.Web Anti-virus for Linux をアンインストールするには以下のコマンドを使用します。

```
yum remove drweb-cc
```

またはグラフィカルマネージャ(PackageKit、Yumexなど)を使ってパッケージをインストール、アンインストールすることも出来ます。

Zypper package manager (SUSE Linux)

リポジトリを追加するには以下のコマンドを実行してください。

```
zypper ar -t YUM http://officeshield.drweb.com/drweb/el5/stable/i386/ drweb
```

または

```
zypper ar -t YUM http://officeshield.drweb.com/drweb/el5/stable/x86_64/
drweb
```

Dr.Web Anti-virus for Linux をインストールするには以下のコマンドを使用します。

```
zypper refresh

zypper install drweb-cc
```

Dr.Web Anti-virus for Linux をアンインストールするには以下のコマンドを使用します。

```
zypper remove drweb-cc
```

または、グラフィカルマネージャ(YaSTなど)を使ってパッケージをインストール、アンインストールすることも出来ます。

キーファイルの取得

インストール終了後、アンチウイルスの使用権利を確定し、アップデート および 常駐アンチウイルス保護 機能のロックを解除するために **Dr.Web Anti-virus for Linux** を登録する必要があります。**Dr.Web Anti-virus for Linux** の初回起動時には、登録は自動的に始まります。または **Register using the serial number** をクリックし、ライセンスマネージャ から登録を開始することも出来ます。

図 11. ソフトウェア登録のライセンスマネージャウィンドウ

必要なオプションを選択し **Continue** をクリックしてください。

オプション	説明
30日間のデモバージョン	デモキーファイルは評価目的で使用され、使用期限が短いため、シリアル番号は必要ありません。
シリアル番号を使用して登録	プログラムに含まれているシリアル番号を指定する必要があります。
既存のキーファイルへのパスを指定	既にコンピューター上に有効なキーファイルを持っている場合にこのオプションを選択します。

上記オプションのうち最初の2つのいずれかを選択した場合、個人情報（名前、メールアドレス、国および都市名）を入力する必要があります。これらの情報は **Doctor Web** がキーファイルを生成する為のみに使用し、第三者には提供され

ません。発行されるキーファイルには、個人を特定するためにこれらの情報が含まれます。詳細については アンチウイルスの登録 を参照してください。

デフォルトでは、ライセンスキーファイルはインストールフォルダに置かれます。 **Dr.Web Anti-virus for Linux** は定期的にファイルを確認します。ライセンスの有効性を保つため、ファイルの編集または変更は行わないでください。

有効なライセンスまたはデモキーファイルが見つからない場合、**Dr.Web Anti-virus for Linux** コンポーネントはブロックされます。プロダクトを登録しキーファイルを受け取る目的でのみ ライセンスマネージャ にアクセス可能です。

チャプター 3. Dr.Web Anti-virus for Linuxの起動

このチャプターでは、 **Dr.Web Anti-virus for Linux** のメイン機能を紹介します。

全てのメイン機能には **Dr.Web Anti-virus for Linux** のウィンドウからアクセス可能です（下図参照）。このウィンドウには、アンチウイルスコンポーネントの管理およびアクセスに必要なセクションが含まれています。

セクション	説明
Dr.Web for Linux	このセクションでは以下のことが可能です。 • **SpIDer Guard** 常駐アンチウイルスコンポーネントを有効/無効にする。詳細については 常駐アンチウイルス保護 を参照してください。 • 最新のアップデートに関する情報を閲覧、必要に応じてアップデートを手動で開始する。詳細については アンチウイルスのアップデート を参照してください。 • **Scanner**、**Quarantine**、**Results**セクションを開く。
Scanner	メインのオンデマンドアンチウイルススキャンコンポーネントにアクセス出来ます。 詳細については オンデマンドでのシステム検査 を参照してください。
Quarantine	隔離 のコンテンツへのアクセスおよびその管理が可能です。 詳細については 隔離の管理 を参照してください。
Results	検出された脅威およびそれらに対して適用されたアクションに関するサマリーを含む、**Dr.Web Anti-virus for Linux** の動作統計へのアクセスおよび閲覧が可能です。 詳細については 結果を見る を参照してください。
Tools	プログラム設定、ログ、および ライセンスマネージャ にアクセス出来ます。
Help	ヘルプおよび参考資料を見ることが出来ます。

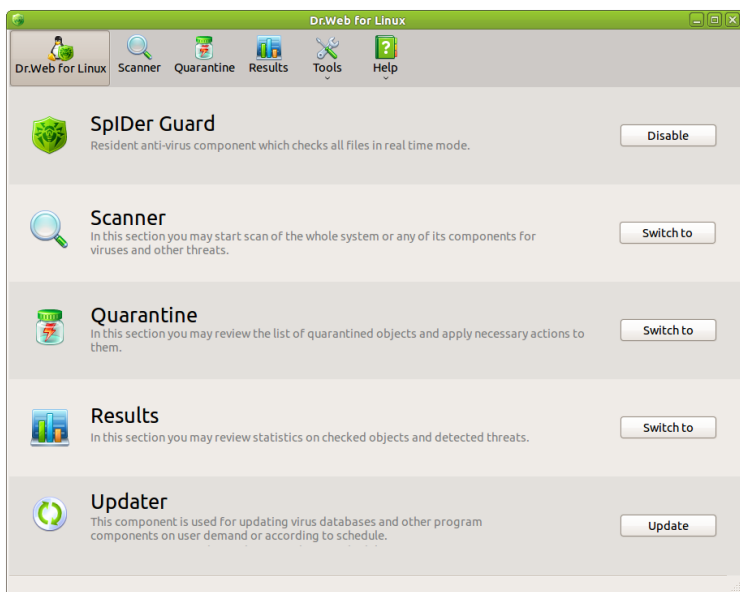



図 12. メインプログラムウィンドウ

アンチウイルスの開始と停止

Dr.Web Anti-virus for Linux を開始するには

以下のいずれかを実行してください。

- **Applications->Dr.Web** メニューを開き、**Dr.Web for Linux** を選択する。
- 以下のコマンドラインでコマンドを実行する。

```
$ drweb-cc
```

Dr.Web Anti-virus for Linux は、起動時に自身を自動ロードリストに加えます。そのため、**Dr.Web Anti-virus for Linux** を停止せずにシステムをシャットダウンした場合、次回のシステム起動時に **Dr.Web Anti-virus for Linux** が自動的に開始されます。

Dr.Web Anti-virus for Linux を停止するには

- 通知領域内の **Dr.Web Antivirus** アイコン を右クリックし、**Quit** を選択します。

Dr.Web Anti-virus for Linux を停止しても、**SpIDer Guard** および **スケジューラ** コンポーネントはアクティブなままです。前者はアクセスのあった全てのファイルを、その度にリアルタイムモードでチェックする常駐アンチウイルスモニターで、後者はスケジュールに沿って検査およびアップデートを開始します（ スケジュールを調整する 参照）。

各ユーザは **Dr.Web Anti-virus for Linux** のそれぞれのコピーを実行および使用することができ、全てのコピーは 同時にまたは別々に 動作します。

アンチウイルスのアップデート

最新の隠ぺい機能を持つ新しい種類のコンピューター脅威が世界中で常に開発され続けています。**Dr.Web Anti-virus for Linux** のコンポーネントおよびウイルスデータベースをアップデートすることで、お使いのコンピューターに対する保護は常に最新のものとなり、新しい脅威に対抗できるようになります。アップデートは、**Updater** と呼ばれる特別なコンポーネントによって実行されます。

Updater を定期的に手動で起動するか（下記参照）、または **Scheduler** を設定して、指定したスケジュールに沿ってプログラムコンポーネントおよびウイルスデータベースをアップデートすることが可能です（ スケジュールの設定 参照）。

Updater を手動で起動するには

以下のいずれかを実行してください。

- **Dr.Web Anti-virus for Linux** メインウィンドウの **Updater** セクション内で **Update** をクリックします。

- 通知領域内の **Dr.Web Antivirus** アイコン を右クリックし、**Update** を選択します。

常駐アンチウイルス保護

常駐アンチウイルス保護は、ユーザまたはシステム内の他のプログラムからアクセスされた、全てのファイルをリアルタイムで検査する **SpIDer Guard** と呼ばれる常駐コンポーネント経由で実行されます。デフォルトでは、**Dr.Web Anti-virus for Linux** をインストール、登録すると同時に有効になります。脅威が検出される度に **SpIDer Guard** が警告を表示し、アンチウイルスプリファレンスに応じてアクションを適用します（ 自動アクションの設定 参照）。

SpIDer Guard を有効または無効にするには

以下のいずれかを実行してください。

- メインウィンドウの **SpIDer Guard** セクションで、**Enable** または **Disable** をクリックします。
- 通知領域内にある **Dr.Web Antivirus** アイコン を右クリックし、**Enable** または **Disable** を選択します。

このオプションを使用する際には次のことに気を付けてください。**SpIDer Guard** 機能が無効になっている間はインターネットへの接続を避け、アクセスする前に スキャナ を使用して全てのリムーバブルメディアを検査してください。

Dr.Web Anti-virus for Linux を終了したとき、**Dr.Web Anti-virus for Linux** は、終了時の **SpIDer Guard** のステータスを保持し（enabled か disabled）、次回 **Dr.Web Anti-virus for Linux** が起動したときに前回のステータスで起動します。**Dr.Web Anti-virus for Linux** を終了する前に **SpIDer Guard** をdisabledに設定した場合は、次回ソフトウェアを起動したときに手動でenabledに設定する必要があります。

SpIDer Guard のモニターは、それを起動したユーザの権限でスキャンを行うよう実装されています。その為、権限不足によりファイルまたはディレクトリへのアクセスが拒否される場合があります。この場合、レポートにアクセスが拒否された旨のメッセージが記録されます。このような状況を回避する為に、アンチウイルスプリファレンス内では、特定のファイルおよびフォルダを **SpIDer Guard** による検査の対象から除外し、1つのファイルに対する検査時間の上限を設定することが可能です（ ファイルを検査対象から除外 参照）。

Increase of inotify subsystem limit

SpIDer Guard ファイルモニターは、リアルタイムにファイルを検査する為に、inotify カーネルモジュールを使用しています。もしinotify の制限値を超えている場合、以下のようなメッセージが **SpIDer Guard** のシステムログに記録されます。

```
drweb-spider: WARNING: inotify limit is exceeded
```

Inotify による制限は、`fs.inotify.max_user_watches` パラメーターで指定されます。現在のこの値を参照するには、以下のコマンドを使用します。

```
# sysctl -a | grep 'fs.inotify.max_user_watches'
```

コマンドを実行すると、以下のように結果が表示されます。

```
fs.inotify.max_user_watches = <digit>
```

`<digit>` の部分が、inotify による制限値です。

- 一時的にこの制限値を増やす場合、以下のコマンドを使用します。

  ```
  # sudo sysctl fs.inotify.max_user_watches=<digit>
  ```

  `<digit>` に入力する値は、現在の `fs.inotify.max_user_watches` パラメーターの値よりも大きくする必要があります。

  この場合、変更は、コンピューターを再起動するまで有効になります。

- 恒久的に制限値を変更する場合は、下記を行ってください。
  1. `/etc/sysctl.conf` に下記を追記してください。

     ```
     fs.inotify.max_user_watches = <digit>
     ```

  2. 変更を有効にするためには、システムを再起動するか、下記のコマンドを実行してください。

     ```
     # sysctl -p
     ```

これらの操作を行うためには、管理者権限 (root) が必要となります。

SELinuxによって保護されているOS

お使いのOSがSELinuxによって保護されている場合、**Dr.Web Scanner** を起動してシステムのウイルス検査を実行しようとすると以下のエラーが表示されます。

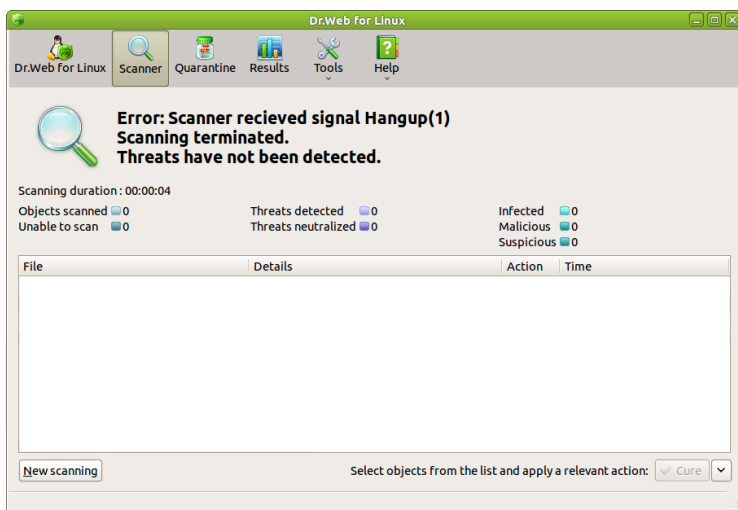



図 13. スキャナエラー

SELinuxによって保護されたOS内で **Dr.Web Scanner** および **Dr.Web Daemon** の正常な動作を設定するには、それらモジュールのポリシーをコンパイルする必要があります。

モジュールポリシーのコンパイルに使用されるテンプレートは、Linuxディストリビューションとそのバージョン、SELinuxポリシーの設定、およびユーザ設定によって大きく異なる場合があります。ポリシーのコンパイルに関する詳細については、お使いのLinuxディストリビューションの該当するマニュアルを参照してください。

必要なポリシーの作成には `policygentool` コマンドを使用することができます。このコマンドは、ポリシーモジュール（インタラクションを調整する必要のある）の名前、および対応する実行ファイルへのフルパスの2つのパラメータを取ります。

例:

`# policygentool drweb-scanner /opt/drweb/drweb.real` - スキャナ

`# policygentool drweb-daemon /opt/drweb/drwebd.real` - Daemon

共通するドメイン特性をいくつか入力するよう促され、各モジュールに対して [module_name].te、[module_name].fc、[module_name].if の3つのファイルが作成されます。

[module_name].te ファイルをコンパイルするには、以下のコマンドを実行してください。

```
checkmodule -M -m -o module-name [module_name].
te
```

ポリシーを正常にコンパイルするには、システムに checkpolicy パッケージがインストールされている必要があります。

要求される（必要な）ポリシーをコンパイルするには以下のコマンドを実行してください。

```
semodule_package -o [module_name].pp -m module-
name
```

新しいポリシーモジュールをモジュールストアにインストールするには以下のコマンドを実行してください。

```
semodule -i [module_name].pp
```

オンデマンドでのシステム検査

オンデマンド検査は **スキャナ** によって実行されます。**スキャナ** は、ユーザの要求またはスケジュールに応じてファイルシステム内のオブジェクトを検査し、システム内に存在する可能性のある様々な脅威を、例えアクティブな状態でなくても検出します。**Dr.Web Anti-virus for Linux** ウィンドウの **スキャナ** セクションを使用して、システム検査を定期的に実行する必要があります。

検査は手動で実行するか（下記参照）、または **スケジューラ** を設定して、指定したスケジュールに沿って実行することができます（スケジュールの設定）。

検査の間はプロセスロードが増大し、バッテリーの減りが早くなる場合があります。検査を実行する際はコンピューターをコンセントに接続することを推奨します。

手動でシステムを検査するには

1. **Dr.Web Anti-virus for Linux** ウィンドウの **スキャナ** セクションを開きます。

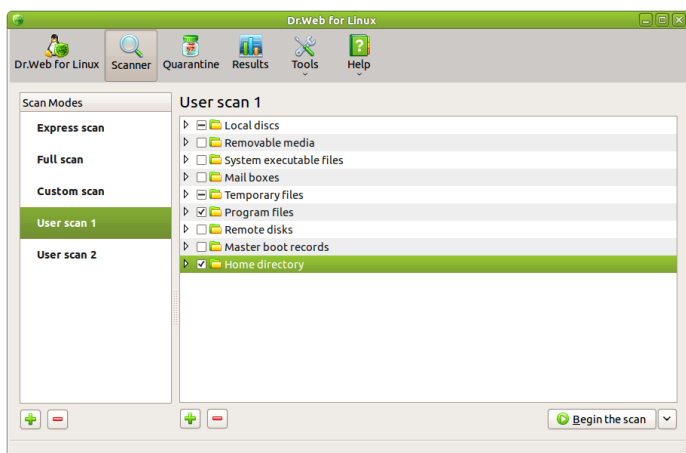



Figure 14. Displaying results of the current check.

2. 検査のモードを選択してください（詳細については、ファイルシステムウィンドウをご覧ください）。
   * **クイックスキャン** – システムの最も脆弱な部分のみを検査します。
   * **フルスキャン** – ファイルシステム全体のフルスキャンを実行します。
   * **カスタムスキャン** – 検査するファイルおよびフォルダを手動で指定します。
   * **ユーザスキャン**（追加された場合）– 前回指定したファイルおよびフォルダを検査します。

   最初の3つのモードはデフォルトで使用することができるようになっています。またそれらは、検査するオブジェクトのセットに関する情報を含んでいることから「検査セット」とも呼ばれます。ユーザスキャンモードを作成することも可能です。新しいモードを追加するには、検査モードのリスト下にある ボタンをクリックし、追加されたモードに名前を付けてください。検査のセット

   はいくらでも追加することができ、必要の無いモードを選択して ボタンをクリックすることで削除することも可能です。

3. **カスタムスキャン** またはユーザスキャンモードを使用する場合、検査したいファイルおよびフォルダをチェックボックスで選択してください。

   リスト下にある ボタンをクリックして他のオブジェクトを追加することが出来ます。オブジェクトを削除したい場合は、該当するオブジェクトを選択して ボタンをクリックします。ユーザスキャンモードを設定した場合、全ての設定が保存され、再度同じモードを選択した際に復元されます（**カスタムスキャン** モードの場合と異なります）。

4. ボタンをクリックし、検出された脅威に対するアクションの適用方法を選択してください。自動での対応が有効になっている場合、スキャナ はアンチウイルスプリファレンス内で 指定された アクションを自動的に適用します。権限が不足している場合には、自動アクションは適用されません。処理を行う前に、手動で権限を増やすことができます。デフォルトでは、検出された脅威ごとに必要なアクションを手動で選択することが出来るようになっています。

5. **スキャナ** セクションの右下部にある **Start** をクリックしてください。検査が開始されると、スキャンプロセスの状態、スキャン中のファイル、検出された脅威などの情報が表示されます。

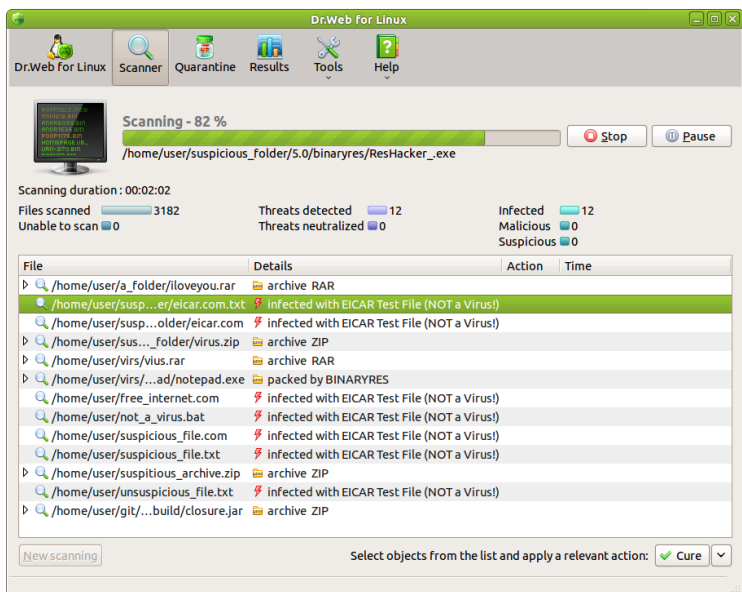



図 15. 検査結果の表示画面

スキャン中の各ステージにおいて、下記のいずれかを実行することができます。

- 処理を中断する為には、**Pause** ボタンを押してください。再開するには、**Continue** ボタンを押してください。
- 処理を中止する為には、**Stop** ボタンを押してください。

スキャンが終了すると、メインウインドウに検出された全ての脅威、もしくは疑わしいファイルが表示されます。手動処理モードで実行した場合、**Scanner** は検出された脅威の情報のみを表示します。

脅威の削除

検査が開始されると、検査プロセスの進行状況、現在検査されているファイルの名前、およびその他の統計情報が表示されます。

検出された全ての脅威の一覧がウィンドウ中央に表示されます。

列	説明
File	検出された、感染したオブジェクトまたは疑わしいオブジェクトへのパス
Details	脅威に関する情報(脅威の種類やウイルス名など)
Action	感染したオブジェクトに適用されたアクションに関する情報(オブジェクトに対していずれのアクションも適用されなかった場合、このフィールドは空になります)
Time	脅威が検出された日付

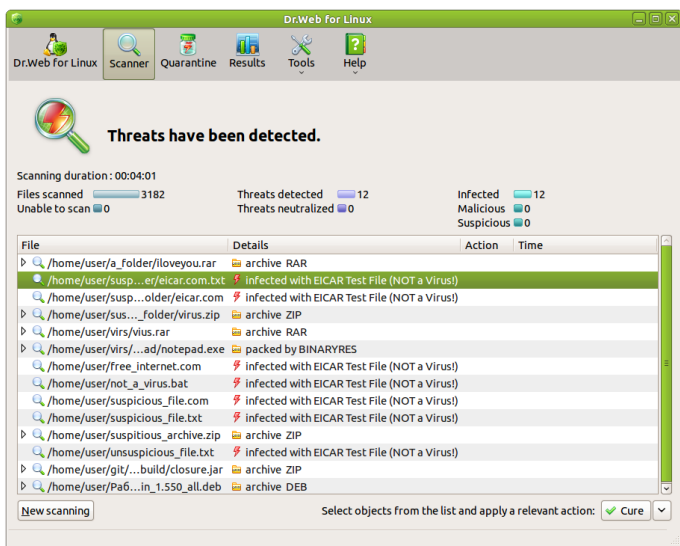



図 16. 検出された脅威の表示

自動プロセスモードでは、スキャナ　は検出された脅威に対して　この設定内で指定した アクションを適用します。

手動プロセスモードでは、スキャナ は検出された脅威についてユーザに通知するだけです。検査終了後に、感染したオブジェクトの正常な機能を復元(*修復*)、またはオブジェクトが修復不可能な場合には脅威を削除(*削除*)することが可能です。

脅威の手動プロセス

1. 脅威(1つの脅威、または同タイプの複数の脅威)に対してアクションを適用するには、リストからオブジェクトを選択してください (複数のオブジェクトを選択するときは、SHIFT キーを押したままCTRL キーで必要なオブジェクトを選択してください)。
2. 以下のいずれかを実行してください。
   * **修復** ボタンをクリックして感染したファイルの修復を試みます。
   * **修復** ボタンの近くにある矢印をクリックし、リストから他のアクションを選択します。
   * オブジェクトを選択してマウスの右ボタンを押し、表示されたメニューから必要なアクションを選択します。

   処理を行うために権限が不足している場合、 **Dr.Web Anti-virus for Linux** は上位権限のユーザで実行するかどうかを確認します。

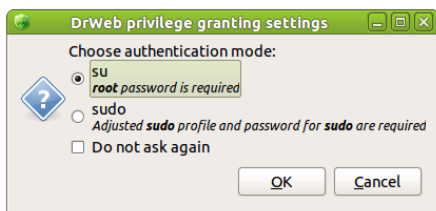



Figure 17. Dr.Web 権限付与設定画面

目的のファイルがウイルスだった場合、**修復** アクションが適用された結果として削除されることがあります。

アクションには以下のような制限があります。

* 疑わしいオブジェクトを修復できない。
* ファイルではないオブジェクト(例:ブートセクター)の隔離、名前の変更、または削除は出来ない。
* アーカイブ、またはコンテナ内の別々のファイルに対して、およびメールメッセージの一部に対してはいずれのアクションも適用できない。この場合、アクションはオブジェクト全体(アーカイブ、コンテナ、メールメッセージ)に対して適用されます。

隔離 に移動した疑わしいファイルを、解析の為に **Doctor Web** に送信することができます。http://vms.drweb.co.jo/sendvirus/ 上にあるフォームを使用してください。

3. アクション適用後、**Dr.Web Anti-virus for Linux** がその結果を **Action** の列に追加します。
4. スキャナ のメインウィンドウに戻るには **New scanning** ボタンをクリックします。

ヘルプについて

プログラムに関するヘルプを見るには **Doctor Web Help** を使用してください。

Dr.Web Helpにアクセスするには

メニューバーで **Help** をクリックし、項目を選択してください。

問題に対する解決、または **Dr.Web Anti-virus for Linux** に関する必要な情報が見つからなかった場合は、テクニカルサポート　に直接お問い合わせください。

チャプター 4. 高度な設定

このチャプターでは、**Dr.Web Anti-virus for Linux** を使用した高度なタスクの実行、およびその設定の調整について説明します。

追加的な機能を使用して、以下の事が可能です。

- アンチウイルス検査の際に **隔離** ディレクトリへ移された疑わしい、または修復不可能なオブジェクトの 処理
- アンチウイルス検査の結果を 閲覧
- 自動スキャン、および **Doctor Web ウイルスデータベース** アップデートの スケジュールを設定
- 定期的な自動スキャンの際に検出された脅威に対して適用する アクションを指定
- 検査の対象から 除外するファイルを指定
- システムイベントに関する 通知を設定

結果の閲覧

Dr.Web Anti-virus for Linux は、スキャナ または **SpIDer Guard** ファイルモニターによって実行された定期的な検査の際にコンピューター上で検出された、悪意のあるオブジェクトやその他の脅威に関する統計を収集します。**Results** セクションでこの統計を閲覧、または必要に応じて古いエントリを削除することが出来ます。

統計を見る

Dr.Web Anti-virus for Linux の動作に関する統計を見るには、メニューバーで **Results** オプションを選択します。

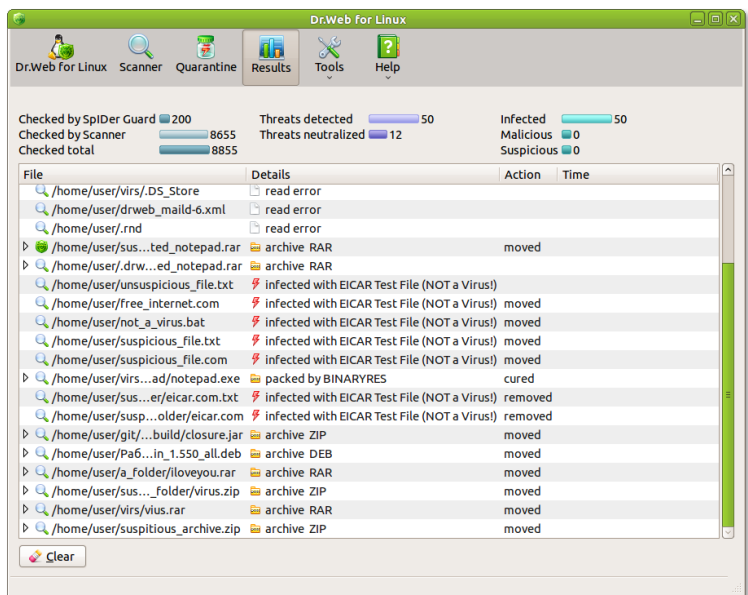



図 18. 検査結果を見る

Results ウィンドウの上部には一般統計が表示されます。

ウィンドウ下部の**Clear** ボタンを押すと、Resultsページからすべてのデータを削除することができます。

ウィンドウの中央には可能性のある、または明らかな脅威の一覧が表示されます。

列	説明
File	パスおよびファイル名
Details	脅威に関する情報（脅威の名前やタイプなど）
Action	検出されたオブジェクトに対して適用されたアクションに関する情報。アクションが適用されていない場合は空になります（下記参照）
Date	脅威が検出された日付

Dr.Web Anti-virus for Linux が集中管理モードで動作している場合、統計情報は集中管理サーバに送信されます。統計情報は以下の場合に送信されます。

- **Clear** ボタンによる送信。この場合、**Result** ページの全てのデータが削除されます。検出された脅威に適用されたアクションとその結果は、スキャンセクションごとに一度だけ集中管理サーバに送信できます。これは、脅威が手動で処理される前に**Clear** ボタンを押すと、検出された脅威と自動的に適用されたアクションに関する情報のみがサーバに送信されることを意味します。
- 集中管理サーバのスケジュールによる統計情報の収集。

隔離の管理

隔離 によって、検出された悪意のあるオブジェクトや疑わしいオブジェクトが修復不可能だった場合に、それらを隔離することが出来ます。修復アルゴリズムは常に改良され続けているため、アップデート後にそれらのオブジェクトが修復可能になる場合があります。

メインウィンドウの **隔離** セクションを使用して 隔離 のコンテンツを閲覧、および管理することが出来ます（下図参照）。

以下の種類のファイルが 隔離 に保存されます。

1. アイコンで示された、一時ファイル。設定（**削除** アクション）によって削除された感染した、または疑わしいファイルのバックアップコピー。必要な場合には、削除されたファイルをこのコピーから復元することが出来ます。
2. アイコンで示された、移動されたファイル。設定（**移動** アクション）によって 隔離 に移された感染した、または疑わしいファイル。修復アルゴリズムは常に改良され続けているため、これらのファイルは後で修復される可能性があります。

1の種類のファイルは設定内で指定された期間だけ 隔離 に保存されます。保存期間が満了すると、ファイルは 隔離 から取り除かれ、永久に削除されます。隔離 に空き容量が無い場合もファイルは削除されます（新しいファイルで上書きされます）。2の種類のファイルは、ユーザの削除処理によってのみ削除できます。。

デフォルトでは 隔離 は、ユーザのホームディレクトリの `.drweb` サブディレクトリにあります。

隔離内にあるオブジェクトを見る

隔離 ウィンドウを開くには、メニューバーで **隔離** オプションを選択します。

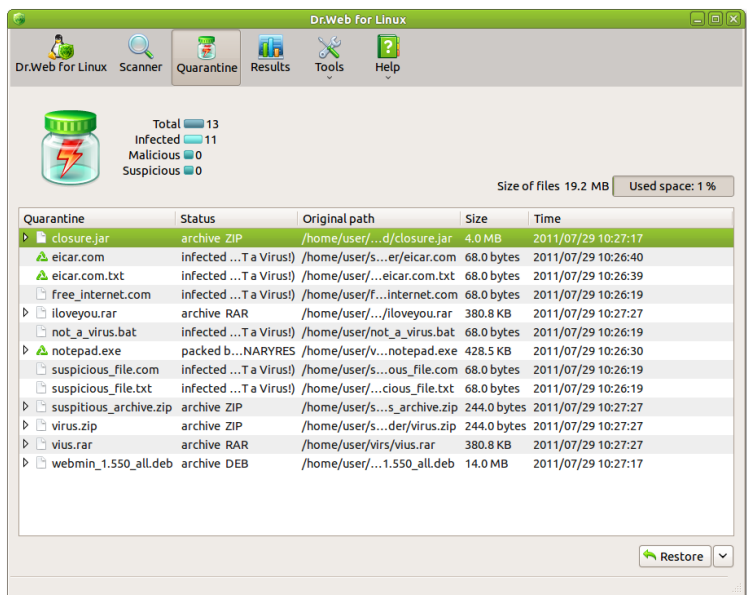



図 19. 隔離ウィンドウ

隔離 ウィンドウの上部には 隔離 内に保存されたオブジェクトに関する一般統計、およびそれらに割り当てられたディスク容量が表示されます。

ウィンドウ中央には 隔離 内に保存されたオブジェクトの一覧が表示されます。

列	説明
Quarantine	パスおよびファイル名
Status	脅威に関する情報（脅威の名前やタイプなど）
Original path	隔離 へ移されたファイルのあったディレクトリへのパス
Date and Time	オブジェクトが 隔離 へ移された日時
Type	オブジェクトをシステム 隔離 、ユーザ 隔離 のどちらに保存するかの指定（システム共通の 隔離 が1つ、および各ユーザごとに別々の 隔離 があります）

隔離内にあるオブジェクトの処理

1. 隔離 内にあるオブジェクトにアクションを適用するには、リストからオブジェクトを選択してください（複数選択する場合は、SHIFTキーを押したままCTRLキーでオブジェクトを選択します）。
2. 以下のアクションのうちいずれかを実行してください。
   - **復元** ボタンを押して、隔離されたファイルをファイルシステム内の元の場所に戻す。
   - **復元** ボタンの近くにある矢印をクリックし、**復元先** を選択してファイルを 隔離 から任意のディレクトリに移す。
   - **復元** ボタンの近くにある矢印をクリックし、**削除** を選択してファイルを 隔離 から削除する。

隔離パラメータの調整

1. **Tools** メニューから **Setting** を選択して **Dr.Web Anti-virus for Linux** の設定画面を開きます。

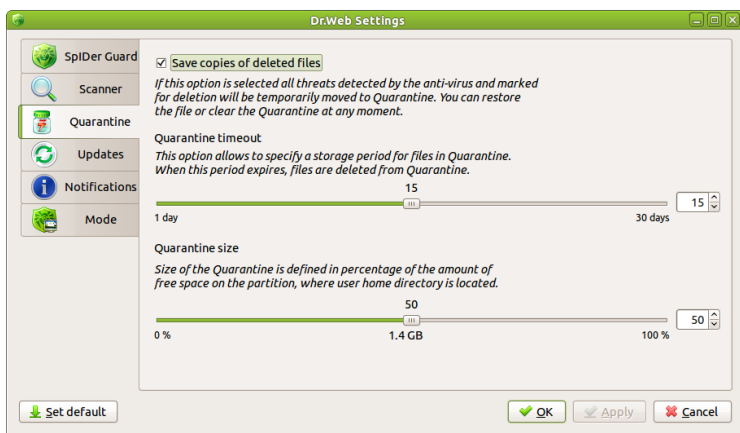



図 20. 隔離設定

2. **隔離** タブを選択します。
3. 隔離 内から削除された、感染したファイルの保存を有効にするには、**Save copies of deleted files** にチェックを入れます。感染したオブジェクトを永久に削除する、およびそれらの 隔離 からの復元を無効にするにはチェックを外してください。削除されたファイルの隔離コピーには アイコンが付きます。

4. 隔離 内にあるオブジェクトの保存期間、および 隔離 自体のサイズ上限を指定します。

隔離 のサイズを指定した場合でも、そのディスクスペースを確保するわけではありません。パーティション上の空き容量を100% 隔離 に割り当てた場合でも、隔離 の現在のサイズは、隔離されたファイルの合計サイズと同じになります。

スケジュールの設定

自動スキャンおよび自動アップデートのスケジュール設定には スケジューラ を使用します。設定はアンチウイルスプリファレンスの **スキャナ** および **アップデート** セクションで行います。

スケジュールに沿った検査を設定するには

1. **Tools** メニュー内で **Setting** をクリックし、**Scanner** を選択して **Scheduler** タブを開きます。
2. 上部にあるチェックボックスにチェックを入れ、検査の時間およびその間隔を指定したいファイルまたはフォルダにチェックを入れます。

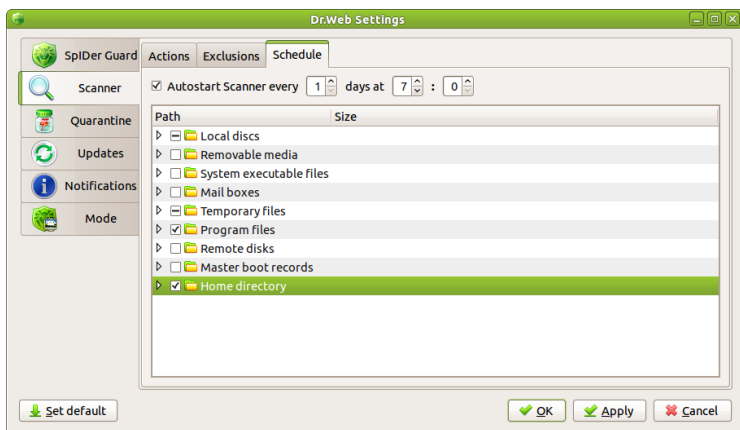



図 21. スキャナのスケジュールタブ

スケジュールに沿ったアップデートを設定するには

1. **Tools** メニュー内で **Setting** をクリックし、ウィンドウ左部で **Update** を選択します。

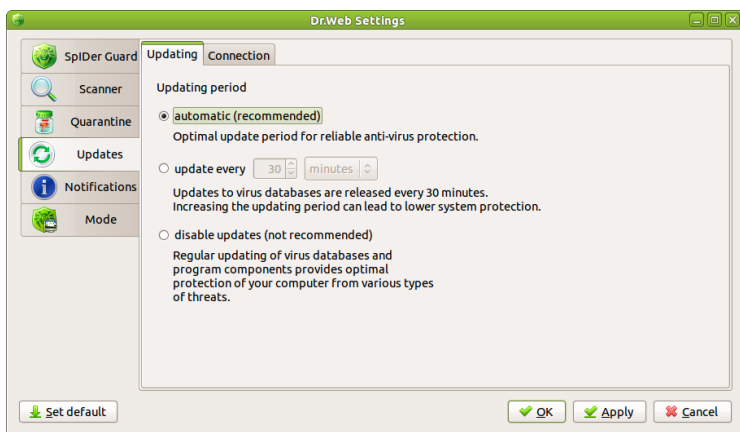



図 22. アップデートタブ

2. 以下のいずれかを選択してください。
   * **Automatic** – 推奨されるデフォルトの間隔でアップデートします。

- **Update every** – アップデートの間隔を指定します。
- **Disable updates** – 自動アップデートを無効にします。このモードで動作させる場合は、**Dr.Web Anti-virus for Linux** を定期的に手動でアップデートしてください。

自動アクションの設定

検出された悪意のあるオブジェクトに対して手動での処理が無効な場合に、脅威に対して自動的に適用するアクションを指定することが出来ます。スキャナ および **SpIDer Guard** に対し個別に設定することが可能です。

その他に以下のアクションを指定することが出来ます。

- **修復** （感染したファイルにのみ使用） - 既知のウイルスに感染したオブジェクトの修復を試みます。ファイルを修復できなかった場合、修復不可能なファイルに対するアクションが適用されます。
- **削除** - 感染した、または疑わしいファイルを削除します。
- **隔離** - 感染した、または疑わしいファイルを 隔離 ディレクトリに移動します。
- **レポート** - 検出された脅威についてユーザに通知します。このアクションが選択されている場合、検出された悪意のあるオブジェクトに対する全ての動作は、手動で行う必要があります。このアクションは、疑わしいファイル、リスクウェア、hacktools、ジョーク等に対してデフォルトとして適用されています。
- **無視** （疑わしいファイル、および全ての種類のリスクウェアに対して使用） - ファイルを通過させます（感染しているファイルについての通知はログに出力されます）。

アクション タブで指定されているデフォルトの設定は、お使いのシステムに対する保護に最適なものとなっています。不必要に変更しないことを推奨します。

自動アクションを設定するには

1. **Dr.Web Anti-virus for Linux** コンポーネントの自動アクション設定を開くには、以下のいずれかを実行してください。
   - スキャナ の自動アクションを設定するには、**ツール** メニュー内で **設定** をクリックし、**スキャナ** を選択して **アクション** タブを開きます。

- **SpIDer Guard** の自動アクションを設定するには、**ツール** メニュー内で **設定** をクリックし、**SpIDer Guard** を選択して **アクション** タブを開きます。

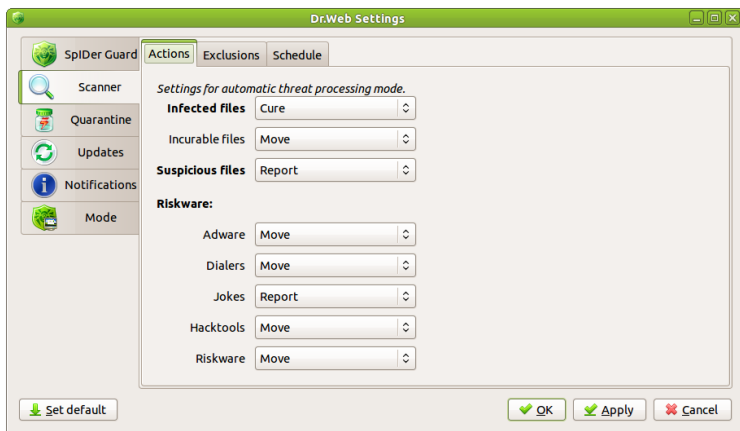



図 23. スキャナのアクションタブ

2. それぞれの脅威に対して必要なアクションを選択します。
3. 必要な設定を全て編集した後、変更を保存するには **OK** を、全ての変更を破棄するには **Cancel** をクリックしてください。

ファイルを検査対象から除外

検査の対象から除外したいファイルおよびディレクトリのリストを作成することが出来ます。**スキャナ** および **SpIDer Guard** で同じ手順を使用します。

隔離 ディレクトリ(通常、ユーザホームディレクトリ内の`/.drweb` サブディレクトリ)へのアクセスはブロックされているため検査の必要が無く、このディレクトリはデフォルトで除外リストに含まれています。

除外 タブのデフォルト設定は、お使いのシステムに対する完全な保護に最適なものとなっています。不必要に変更しないことを推奨します。

除外リストの設定

1. **Dr.Web Anti-virus for Linux** コンポーネントの除外設定を開くには、以下のいずれかを実行してください。
    - **SpIDer Guard** の除外リストを設定するには、**Tools** メニュー内で **Settings** をクリックし、**SpIDer Guard** を選択して **Exclusions** タブを開きます。
    - **スキャナ** の除外リストを設定するには、**Tools** メニュー内で **Settings** をクリックし、**Scanner** を選択して **Exclusions** タブを開きます。

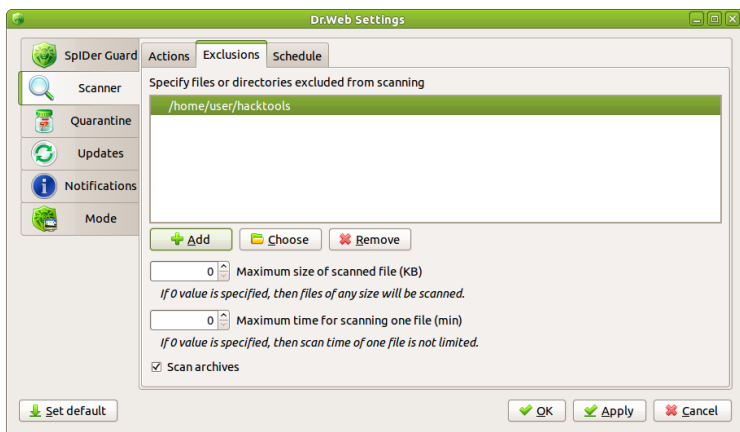
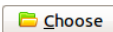



図 24. スキャナの除外タブ

デフォルトでは、検出された脅威を隔離するために使用されるフォルダであり、検査しても意味がなく、アクセスがブロックされているとして、**Quarantine** フォルダはどちらのコンポーネントのスキャンからも除外されています。

2. 必要に応じ、除外するファイルのリストを変更します。

- ファイルまたはフォルダをリストに追加するには、 Add ボタンをクリックしてオブジェクトを選択します。選択を変更するには Choose をクリックしてください。
- 全ての種類のアーカイブを除外するには、**Scan archives** フラグを無効にしてください。
- **SpIDer Guard** では、1つのファイルに対する検査時間の上限を指定し、常駐モニターが破損したファイルの検査に時間をかけないようにすることが出来ます。
- スキャナ では、検査されていないファイルの、検査結果内での表示を設定することが出来ます。

3. 必要な設定を全て編集した後、変更を保存するには **OK** を、全ての変更を破棄するには **Cancel** をクリックしてください。

通知の設定

Dr.Web Anti-virus for Linux は、その動作中に起こる様々なイベントに関してユーザに通知をすることが出来ます。

通知には以下の2種類があります。

- **SpIDer Guard** によって画面上に表示されるメッセージ
- スキャナ および **SpIDer Guard** による警告音

スキャナの通知を設定

1. **Tools** メニュー内で **Settings** をクリックして **Notifications** を選択します。

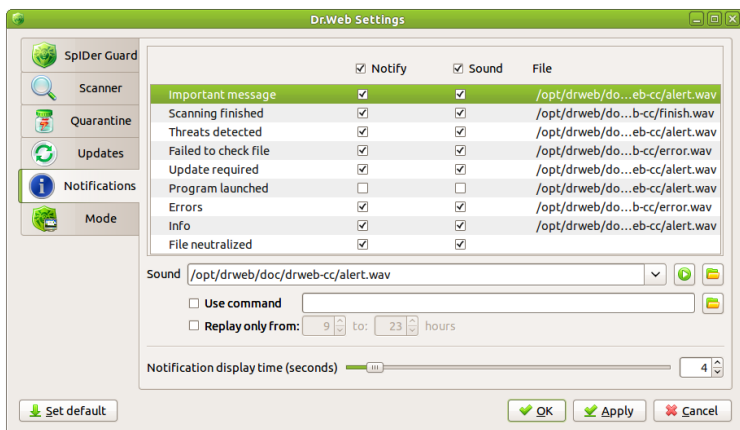



図 25. 通知タブ

2. 必要に応じ、警告音の設定を変更してください。
   - 警告音を有効／無効にするには、タブ上部にある **Sound** チェックボックスを選択／クリアしてください。
   - 特定のイベントに対して警告音を有効／無効にするには、**Sound** カラム内の該当するチェックボックスを選択／クリアしてください。
   - イベントに対して特定の音を設定するには、イベントを選択し **Sound** リスト内から音を指定してください。他の音をリストに追加するには、**Choose** をクリックして音声ファイルを選択します。警告音を再生する特別なコマンド、および警告音を有効にする時間間隔を指定することも可能です。選択したファイルを再生するには **Play sound** ボタンをクリックします。
3. 必要に応じ、画面上に表示される通知の設定を変更してください。
   - スライダーを使用して、メッセージを画面上に表示し続ける時間を設定します。
   - 画面上の通知表示を有効／無効にするには、タブの上部にある **Notify** チェックボックスを選択／クリアしてください。
   - 特定のイベントに関する画面上の通知表示を有効／無効にするには、**Notify** カラム内の該当するチェックボックスを選択／クリアしてください。

複数のユーザーによる Dr.Web Anti-virus for Linux の同時使用

1台のコンピューター上で異なるユーザがそれぞれの **Dr.Web Anti-virus for Linux** のコピーを起動・使用することができ、それらは全て同時に、また別々に動作することが可能です。

各ユーザの **Dr.Web Anti-virus for Linux** 初回起動時に、以下のファイルおよびディレクトリがユーザホームディレクトリ(~/.drweb)内に作成されます。

- **Doctor Web スキャナ** のユーザ設定が保存されている、メイン設定ファイル drweb32.ini のコピー
- 特定のユーザに対する設定が保存される **SpIDer Guard** および **Dr.Web Antivirus for Linux** コンポーネントの(drweb-spider.conf および drweb-cc.conf に対応した)設定ファイルのコピー
- ライセンスキーファイル /opt/drweb/drweb32.key へのシンボリックリンク(このファイルの有る無しに関わらず)。指定された場所にこのファイルが有る場合、デフォルトで全てのユーザがファイルを利用することができます。それ以外の場合、ユーザは ライセンスマネージャ 経由でライセンスキーファイルを取得するよう促されます。
- **Doctor Web エンジン** /var/drweb/lib/drweb32.dll へのシンボリックリンク。定期的なアップデートが数回行われた後に、このシンボリックリンクは アップデーター モジュールによって本物の drweb32.dll ファイルと置き換えられる場合があります。
- **SpIDer Guard** および **Control Center** のソケット
- ユーザウイルスデータベースおよび一時ファイルが保存されるディレクトリ、および 隔離 ディレクトリ

動作モードの設定

I必要に応じ、**Dr.Web Anti-virus for Linux** を使用して、**Dr.Web Enterprise Security Suite** で管理された企業ネットワークに接続する、 そのような集中管理モードで動作させる為に、追加のソフトウェアをインストールする必要も、**Dr.Web Anti-virus for Linux** アンインストールする必要もありません。

集中管理モードを使用するには

1. 会社、 アンチウイルスネットワーク管理者に連絡し、パブリックキーファイルおよび集中管理サーバへの接続パラメータを入手してください。
2. **Tools** メニュー内で **Settings** をクリックして **Mode** を選択します。
3. 会社、集中管理サーバに接続する為に、**Use central protection server** を選択してください。

   集中管理モードでは、手動での起動およびアップデート設定のオプションはブロックされています。**Dr.Web Anti-virus for Linux** のいくつかの機能および設定、特に常駐保護やオンデマンド検査に関するものは、企業のセキュリティポリシーに準拠して、変更される場合があります。このモードで動作するための キーファイル は集中管理サーバから受け取ります。個人キーファイルは使用できません。

4. **Dr.Web Anti-virus for Linux** は集中管理モードに切り替えられると同時に、前回の接続パラメータを復元します。サーバへの初回接続時や、接続パラメータが変更されている場合には以下の手順を実行してください。
   - アンチウイルスネットワーク管理者に提供された、集中管理サーバのIPアドレスを入力。
   - サーバへの接続に使用するポート番号を入力。
   - パブリックキーファイルを設定ウィンドウにドラッグ、またはパブリックキーエリアをダブルクリックして参照内からファイルを選択。
   - オプションとして、認証パラメータ(サーバでの登録用に、お使いのコンピューターに割り当てられたステーションID、およびパスワード)を入力。入力した値はシステムキーチェーンに保存されるため、サーバへの再接続の際にそれらを再度入力する必要はありません。

スタンドアローンモードを使用するには

1. **Tools** メニュー内で **Settings** をクリックして **Mode** を選択します。
2. スタンドアローンモードに切り替える為に、**Use central protection server** チェックボックスをクリアしてください。

   このモードに切り替わると同時に、**Dr.Web Anti-virus for Linux** の全ての設定はロック解除され、前回の値またはデフォルト値に復元されます。ユーザは、アンチウイルスの全ての機能にアクセスすることが可能になります。

3. スタンドアローンモードでの正常な動作のために、有効な個人 キーファイル が必要です。このモードでは集中管理サーバから受け取ったキーファイルは使用できません。必要な場合、 ライセンスマネージャ を使用して個

人キーファイルを受け取る、またはアップデートすることが可能です。

ライセンスマネージャの使用

ライセンスマネージャ　は、キーファイルの管理を簡易化するためのコンポーネントです（ ライセンスキーファイル 参照）。キーファイルは アップデート 、常駐保護 、オンデマンド検査　機能をアンロックしてしまうため、製品インストール終了後にインストールしてください。キーファイルを受け取っていない、またはその期限が切れている場合、 ライセンスマネージャ を使用して新しいキーファイルを取得することができます。

ライセンスマネージャを開くには

Tools メニュー内で **License Manager** をクリックします。

ライセンスマネージャ　ウィンドウでは、現在お持ちのキーファイルに関する詳細を表示し、以下のライセンス管理オプションを使用することができます。

オプション	説明
30日間のデモバージョン	デモキーファイルは評価目的で使用され、使用期限が短いため、シリアル番号は必要ありません。
シリアル番号を使用して登録	プログラムに含まれているシリアル番号を指定する必要があります。
既存のキーファイルへのパスを指定	既にコンピューター上に有効なキーファイルを持っている場合にこのオプションを選択します。

ライセンスキーファイル

Dr.Web Anti-virus for Linux の使用に関する権利は、ライセンスキーファイルによって制御されています。

ライセンスキーファイルには以下の情報が含まれています。

- アンチウイルスライセンスの有効期限
- 使用を許可されたコンポーネントのリスト
- その他の制限事項（アプリケーションの使用を許可するユーザの数など）

ライセンスキーファイルは.keyを拡張子を持ち、**Dr.Web Anti-virus for Linux** の初回起動時に ライセンスマネージャ 経由で受け取ることが出来ます。

- デモキーファイルを用いて評価を行うことが出来ます。デモキーファイルでは、主要なアンチウイルスコンポーネントの全ての機能をお使いいただけますが、使用期限があります。
- ライセンスキーファイルを入手するには、製品のシリアル番号が必要です。**Dr.Web** アンチウイルス製品、またはそのシリアル番号は弊社 パートナー または オンラインストア 経由で購入することが出来ます。

ライセンスキーファイルは、.key拡張子を持ったファイル、またはそのようなファイルを含むzipファイルで提供されます。

ユーザの権利を指定するキーファイルのパラメータは、ライセンス同意に応じて設定されます。ファイルにはユーザおよび販売者の情報も含まれています。

ライセンスキーファイルの期限が切れた後に **Dr.Web Anti-virus for Linux** の使用を継続するには、新しいキーファイルを入手し、古いものと置き換える必要があります（-キーファイルの取得 参照）。

ライセンスの登録と更新

デフォルトでは、キーファイルは /home/<user name>/.drweb に保存されています。**Dr.Web Anti-virus for Linux** は定期的にファイルを確認します。ライセンスの有効性を保つため、ファイルの編集または変更は行わないでください。

デモキーファイルが見つからない、またはライセンス期限が切れている場合、ライセンスを更新するかまたは新しいライセンスを取得するまで全てのコンポーネントはブロックされます。

ライセンスマネージャ によって、ファイルから前回受け取ったライセンスをインストール、またはインターネット経由で新しいライセンスを取得することで **Dr.Web Anti-virus for Linux** の使用を登録することができます。

ライセンスマネージャ からの登録を開始するには、**Get new license** をクリックします。 **Dr.Web Anti-virus for Linux** の初回起動時には、自動的に開始されます。

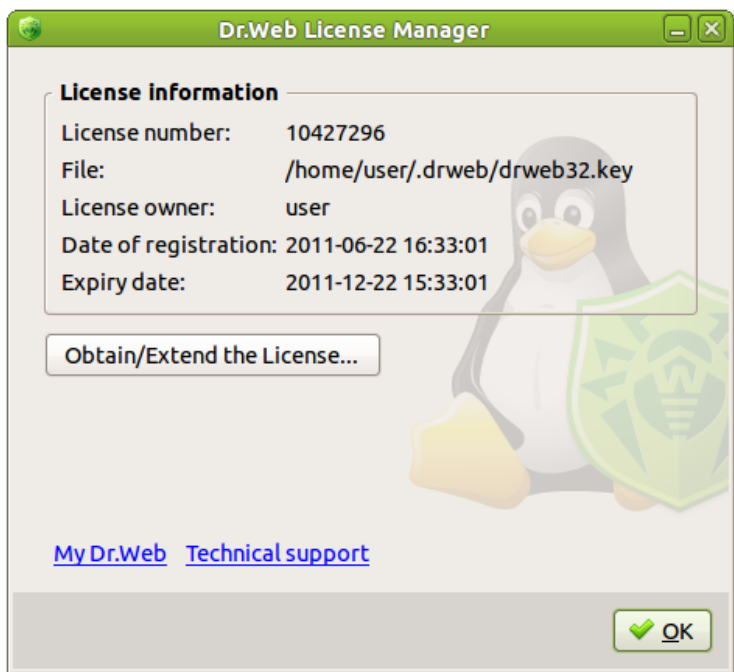



図 26. ライセンスマネージャメインウィンドウ

既存のキーファイルをインストールするには

1. 登録手順1つ目のステップで、**Specify path to an existing key file** を選択します。
2. キーファイルを選択します。キーファイルをアーカイブ内に受け取った場合は、アーカイブを選択します。

   Dr.Web Anti-virus for Linux が新しいキーファイルを使用するように自動的に切り替わります。

新しいキーファイルを取得するには

1. 登録手順1つ目のステップで以下のいずれかを実行します。
   * 登録シリアル番号を持っている場合、**Register using the serial number** を選択し **Next** をクリックします。

- 評価目的で **Dr.Web Anti-virus for Linux** をインストールした場合、**Demo version for 30 days** を選択し **Next** をクリックしてステップ4へ進みます。

図 27. 登録種別画面

2. ライセンスキー取得のためのシリアル番号を入力し **Next** をクリックします。

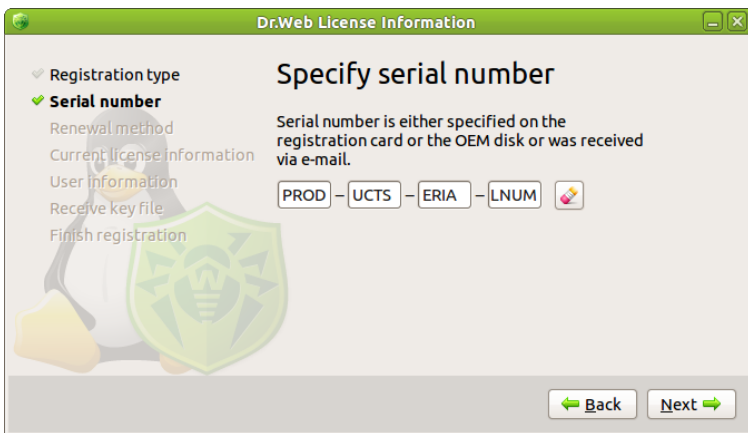



図 28. シリアル番号入力画面

3. シリアル番号を指定、またはキーファイルをアップロードした後、**新しいライセンス** と **更新ライセンス** のどちらであるかを **Dr.Web** ライセンスサーバ

が判別します。

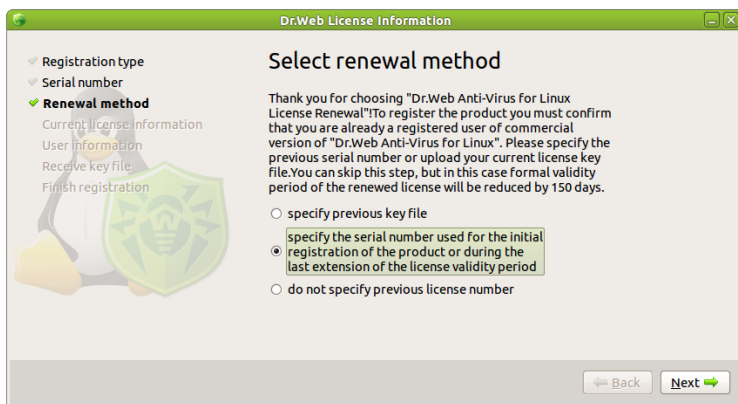



図 29. 新しいライセンスの更新方法選択画面

既に **Dr.Web Anti-virus for Linux** のユーザであり、新しいライセンスを登録する場合、新しいライセンスの有効期限に150日追加することができます。新しいライセンスの有効期限に150日を追加する為に、更新ライセンスを登録するときは、前回のライセンスキーファイルを提出してください。

Next をクリックします。

前回のシリアル番号を指定するか、現在お持ちのライセンスキーをアップロードしてください。

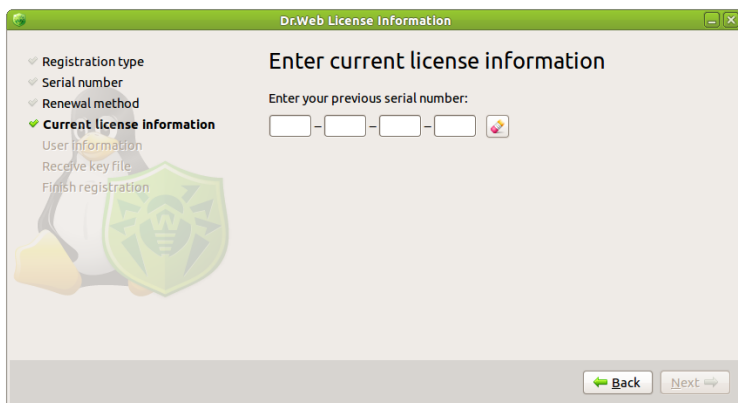



図 30. 前回のシリアル番号入力画面

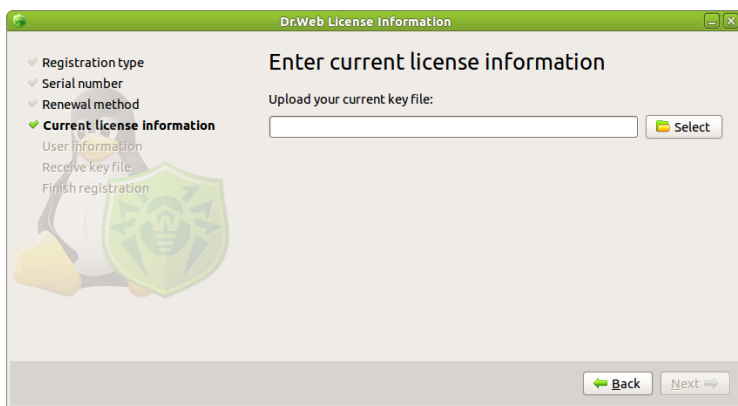



図 31. 現在お使いのライセンスキーファイルアップロード画面

do not specify previous licence number を選択した場合、更新割引が適用されない旨の警告メッセージが表示されます。

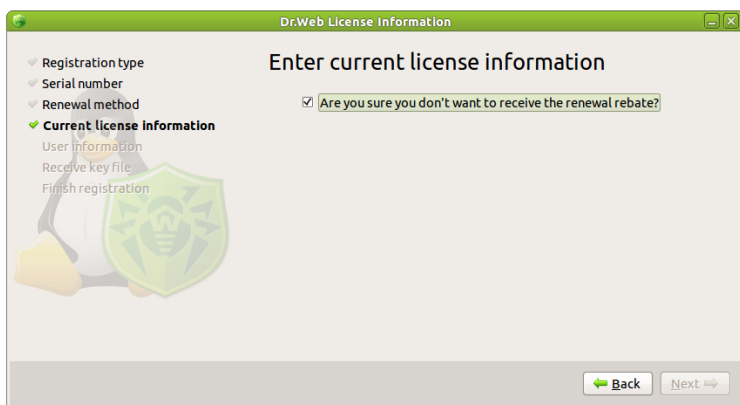



図 32. 警告ウィンドウ

4. キーファイルを受け取るには、個人情報（姓名、メールアドレス）を入力し、国および都市名を選択してください。入力フィールドは全て必須です。Doctor Web に関するニュースをメールで受け取る場合、該当するチェックボックスにチェックを入れてください。
5. キーファイルをダウンロード・インストールするには **Next** をクリックします。インストール実行時は、通常特別な作業を必要としません。キーファイルの取得が正常に行われた場合、**Dr.Web Anti-virus for Linux** は新しいキーファイルを使用し自動的に起動します。

Figure 33. Registration Finish window

ダウンロードに失敗した場合、アップデータ がエラーに関する情報を提供します。

インターネット接続を確認し、再試行してください。

キーファイルは有効期限が満了するまで保管しておくことを推奨します。製品を再インストール、または複数のコンピューター上にインストールする場合に、前回登録したライセンスキーファイルを使用することが出来ます。

シリアル番号を使用してキーファイルを取得した場合、起動時に以下のような警告メッセージが表示されます。

```
ERROR: Dr.Web ® Updater: key file not found !
See Dr.Web ® Updater log file for details.
```

この通知を無効にするには、To disable this notification, comment out the line in /etc/cron.d/drweb-update にある、Updaterを読みだす下記の記述をコメントアウトします。

```
# */30 * * * * drweb /opt/drweb/update.pl
```

2回目以降の登録

キーファイルを紛失した場合は再度登録する必要があります。その際には、前回の登録時と同じ個人情報を入力してください。メールアドレスは別のものを使用することが可能です。その場合キーファイルは指定されたアドレスに送信されます。

デモキーファイルを再発行する場合、前回登録時と同じキーファイルが発行されます。同一のコンピューターに対するデモキーファイルの再発行は4か月に1回のみとなります。

キーファイルの請求回数には制限があり、同じシリアル番号を登録できるのは25回までです。その回数を超えて請求されてもキーファイルは送信されません。その場合は、シリアル番号と、シリアル番号を登録時に登録した個人情報とともに、現象の詳細を テクニカルサポート にご連絡ください。

集中管理

Doctor Web の集中管理ソリューションは、論理構造内にあるコンピューター(例えば、企業ローカルネットワーク内外からお互いにアクセスする企業のコンピューターなど)の情報セキュリティの設定および管理を自動化・簡易化します。保護されるコンピューターは、管理者が集中管理サーバからそのセキュリティを監視および

管理するアンチウイルスネットワーク内で1つに統合されます。集中管理されているアンチウイルスシステムへの接続によって、エンドユーザによる操作を最小限に抑えると同時にレベルの高い保護を保証します。

アンチウイルスネットワークの論理構造

Doctor Web の集中管理はクライアントサーバモデルを使用します（下図参照）。

ワークステーションとサーバはインストールされた *ローカルアンチウイルスコンポーネント*（エージェントまたはクライアント、本マニュアルでは **Dr.Web Anti-virus for Linux** ）によって保護され、それによってリモートコンピューターに対するアンチウイルス保護を提供し、集中管理サーバ への容易な接続を確かなものにします。

ローカルコンピューターのアップデートおよび設定は *集中管理サーバ* から行われます。アンチウイルスネットワーク内の指令、データおよび統計情報もまた集中管理サーバを経由します。保護するコンピューターと集中管理サーバ間のトラフィックは非常に大きくなる可能性があるため、圧縮のオプションを使用することが出来ます。機密情報の漏洩やダウンロードしたソフトウェアのすり替えを回避する為、暗号化にも対応しています。

必要な全てのアップデートは **Dr.Web Global Update System** サーバから集中管理サーバにダウンロードされます。

ローカルアンチウイルスコンポーネントは、*アンチウイルスネットワーク管理者* からのコマンドに応じて集中管理サーバから設定および管理されます。管理者は集中管理サーバ、およびアンチウイルスネットワークトポロジーを管理し（リモートコンピューターから集中管理サーバへの接続を有効にするなど）、必要な場合はローカルアンチウイルスコンポーネントの動作を設定します。

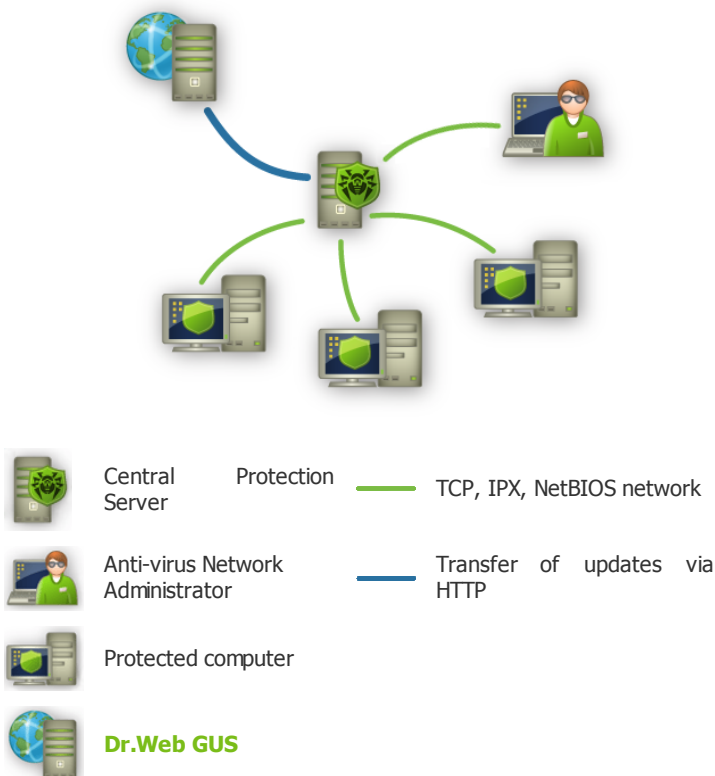



図 34. アンチウイルスネットワークの論理構造

集中管理ソリューション

Dr.Web® Enterprise Suite

Dr.Web® Enterprise Suite は、あらゆる規模の企業ネットワークに対する複合的なソリューションで、全ての種類のコンピュータ脅威からワークステーション、メールおよびファイルサーバを確実に保護します。またこのソリューションによって、アンチウイルスネットワーク管理者にはコンポーネントの展開とアップデート、ネットワークステータスの監視、統計情報の収集、およびウイルスイベントに関する通知を含

むローカルアンチウイルスコンポーネントの動作を追跡、管理することを可能にする様々なツールが提供されます。

集中管理モードの設定

必要に応じ、インストールした **Dr.Web Anti-virus for Linux** アンチウイルスソリューションを使用して、**Dr.Web® Enterprise Suite** によって保護された企業ネットワークに接続することが可能です。そのような集中管理モードで動作させるために追加のソフトウェアをインストールしたり、**Dr.Web Anti-virus for Linux** をアンインストールする必要はありません。

Dr.Web Agent を集中管理モードで起動させるには、drweb-agent-es パッケージがインストールされている必要があります。

集中管理モードを使用するには

1. アンチウイルスネットワーク管理者に連絡し、パブリックキーファイルおよび集中管理サーバに接続する為のパラメータを入手してください。
2. **Tools** メニューの **Settings** アイテムを選択して設定画面を開きます。
3. **Mode** タブを選択します。

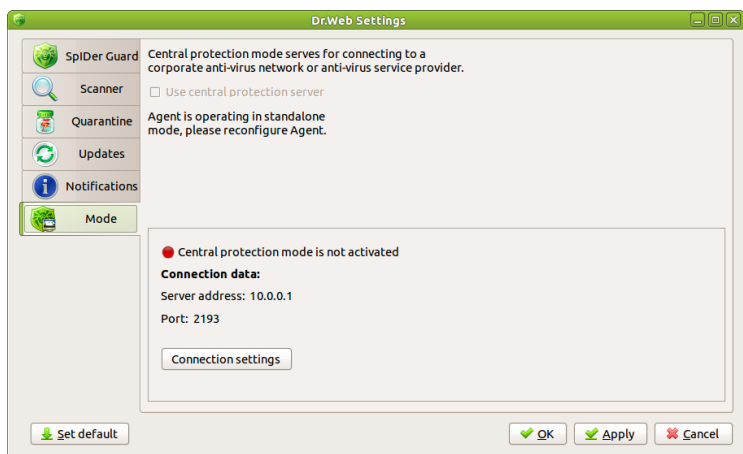



図 35. "Mode" タブ

1. 会社の集中管理サーバに接続する為に、**Use central protection server** チェックボックスを選択してください。
2. 集中管理モードに切り替わると、**Dr.Web Anti-virus for Linux** は前回の接続パラメータを復元します。サーバへの初回接続時や接続パラメータが変更されている場合は以下の手順を実行してください。
   - **Connection Settings** ボタンをクリックし、集中管理サーバとの接続を確立するためのパラメータ設定のウィンドウを開きます。

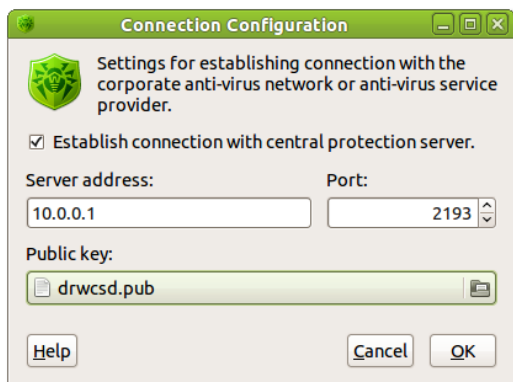



図 36. 接続調整設定

- 集中管理サーバの IP アドレスを入力します。
- サーバに接続する為のポート番号を入力します。
- パブリックキーエリアをダブルクリックし、必要なファイルを参照内から選択してパブリックキーファイルを指定します。

3. 他のサーバに接続したい場合は、以下を行ってください。
   - **Connection Settings** ボタンをクリックします。表示されたウィンドウで、項目5のような新しい接続パラメータを設定します。OKを押して設定を保存します。
   - 再度Connection　Settingsウィンドウを開き、設定が保存されていることを確認します。　問題なければOKを押してください。これ以降、設定が有効になります。

接続設定を変更するには、管理者権限が必要です。通常、suのrootパスワードを、もしくはsudoのユーザーパスワードを指定します(sudo　のユーザープロファイルが正確に設定されている場合）。GNU/Linuxベースの他のOSでは、モード／パスワードの別の組み合わせが使用される場合があります（例えば、**sudo** に `root` パスワードを使用するなど）。

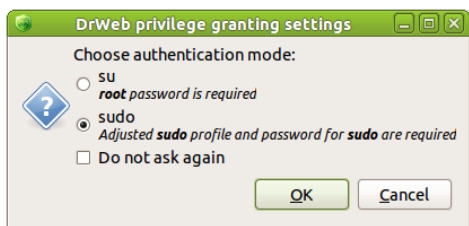



Figure 37. Selecting authentication method.

集中管理モードでは、企業のセキュリティポリシーに準拠して、または購入したサービスのリストに応じて **Dr.Web Anti-virus for Linux** のいくつかの機能および設定が変更・ブロックされる場合があります。このモードでの動作に必要なキーファイルは集中管理サーバから受け取ります。個人キーファイル は使用できません。

集中管理サーバ上での新アカウント作成

Dr.Web Anti-virus for Linux アンチウイルスソリューションと集中管理サーバ間の連携は **Dr.Web Control Agent** コンポーネント経由で行われます。サーバとの接続が確立 されると、対応する変更が エージェント の設定ファイルに対して自動的に適用されます。

新しいワークステーションはその接続ポリシーに応じて、異なる2つの方法で集中管理サーバに接続することができます。

- 新しいアカウントをサーバが自動的に作成する場合
- 上記アカウントを管理者が手動で作成する場合

新しいアカウントを自動的に作成する場合

1. エージェント は集中管理モードでの初回起動時に、アカウントの詳細（ステーションIDおよびパスワード）要求をサーバに送信します。
2. 集中管理サーバが `Approve access manually` モードに設定されている場合、webインターフェース経由での新しいステーションの登録をシステム管理者が承認する必要があります。
3. 初回起動後に エージェント はステーションIDおよびパスワードのハッシュを特別なファイル（デフォルトパスは `/var/drweb/agent/pwd`）に記録します。暗号化キーには エージェント が動作しているホスト名が使用されます。

4. このファイルのデータは **Dr.Web Anti-virus for Linux** が集中管理サーバに接続する度に使用されます。
5. パスワードファイルを削除した場合、次回の エージェント 起動時に登録要求が再度サーバに送られます。

新しいアカウントを手動で作成する場合

1. 集中管理サーバ上で新しいアカウントを作成します。ステーションIDは自動で生成され、パスワードは手動で指定します。
2. 接続設定 ウィンドウ内の該当するフィールドでログイン(ステーションID)とパスワードを指定してください。

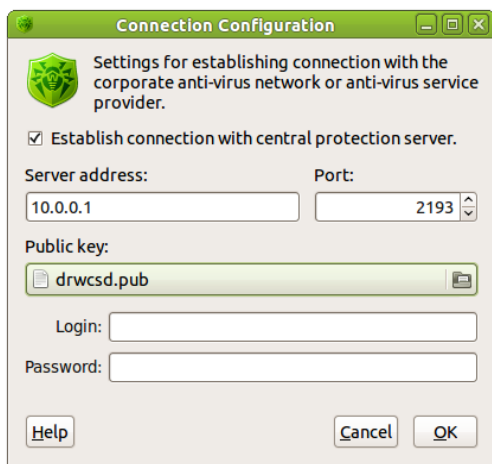



図 38. 接続設定の調整

エージェント はステーションIDおよびパスワードのハッシュを特別なファイル(デフォルトパス `/var/drweb/agent/pwd`)に記録します。暗号化キーには エージェント が動作しているホスト名が使用されます。

3. このファイルのデータは **Dr.Web Anti-virus for Linux** が集中管理サーバに接続する度に使用されます。
4. パスワードファイルを削除した場合、再度登録を行う必要があります。

集中管理サーバのWebインターフェース経由でコンポーネントを設定する

Anti-virus networks operated by **Dr.Web Enterprise Security Suite** によって構築されたアンチウイルスネットワークでは、下記のようにワークステーションのアンチウイルス設定を一元的に管理できます。

- アンチウイルスプログラムのパラメータの設定
- ワークステーションのタスクのスケジュール設定
- スケジュール設定に従ってコンピュータのスキャンを実行する
- ワークステーションの更新、またはアップデート後のエラーは、再起動することでステータスがリセットされます。

Every time **Dr.Web Anti-virus for Linux** が起動する度に、**Agent** は、集中管理サーバーから**Dr.Web for Linux** ソフトウェアの包括したコンポーネントの設定、および **Dr.Web SpIDer Guard** アンチウイルスコンポーネントを受け取ります。そのため、それらのコンポーネントの設定は、集中管理サーバのwebインターフェース経由で行うことができます。

Dr.Web ESS の用語では、**Dr.Web Anti-virus for Linux** は **Dr. Web Scanner for Linux.** と表記されることにご注意ください。

Dr.Web Scanner および **Dr.Web SpIDer Guard** コンポーネントの設定を変更するための十分な権限をユーザが持っている場合、**Dr.Web Anti-virus for Linux** インターフェース 経由で行われた全ての変更は自動的に集中管理サーバへエクスポートされます。

一時的に**Server** との接続が切断されている場合、ワークステーションの設定変更を行うことができます。**Server** との接続が加速的速やかに回復することを前提に、ワークステーションによって受け入れられます。

スタンドアロンモードの設定

スタンドアローンモードに切り替えることで **Dr.Web Anti-virus for Linux** を **Dr.Web® Enterprise Suite** が保護する企業ネットワークから切り離すこと

が出来ます。

スタンドアローンモードを使用するには

1. 会社のアンチウイルスネットワーク管理者に連絡し、集中管理サーバからの接続を切るための許可を得てください（必要な権限をサーバのwebインターフェース経由でユーザに付与する必要があります）
2. **Tools** メニューの **Settings** アイテムを選択して設定画面を開きます。
3. **Mode** タブを選択します。

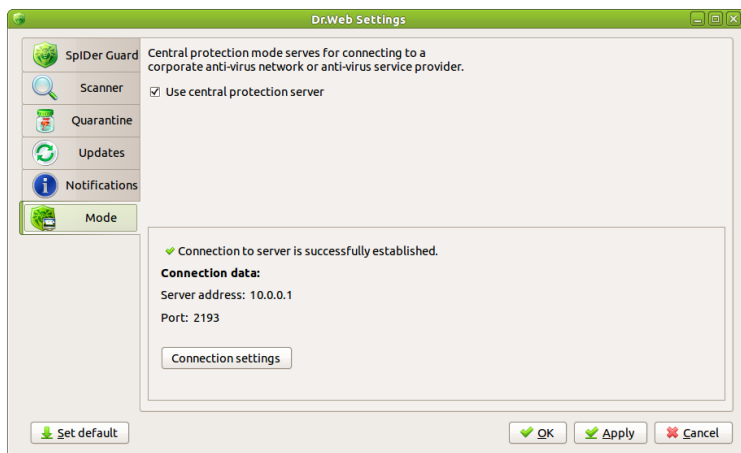



図 39. "Mode" タブ

4. スタンドアローンモードに切り替える為に **Use central protection server** チェックボックスのチェックを外してください。
5. このモードに切り替わると同時に、**Dr.Web Anti-virus for Linux** の全ての設定はロック解除されます。ユーザは再びアンチウイルスの全ての機能にアクセスすることが可能になり、 アップデート を手動で設定および実行、**SpIDer Guard** を 管理 することが出来るようになります。

   スタンドアローンモードでの正常な動作のために、有効な個人 キーファイル が必要です。このモードでは集中管理サーバから受け取ったキーファイルは使用できません。必要な場合、 ライセンスマネージャ を使用して個人キーファイルを受け取る、またはアップデートすることが可能です。

スタンドアロンモードの追加設定

集中管理サーバとの接続確立設定が調整されると、いくつかの **Dr.Web Anti-virus for Linux** コンポーネント(**Dr.Web Monitor** および **Dr.Web Agent**)の設定ファイルが変更されます。該当するファイル monitor.conf および agent.conf - は /etc/drweb/ ディレクトリに保存されます。

Dr.Web Monitor の場合

設定ファイル[Monitor] セクションの **RunAppList** パラメータ値が変更され、モニター によって起動されたモジュールのリストに エージェント モジュールが追加されます(AGENT 値)。

Dr.Web Agent の場合

設定ファイル [EnterpriseMode] セクションの **UseEnterpriseMode** パラメータ値が Yes に変更され、集中管理サーバのホスト名が **ServerHost** パラメータ内で、ポート番号が **ServerPort** パラメータ内で指定されます。

そのため、**Dr.Web Anti-virus for Linux** をスタンドアローンモードに切り換えると、それらのパラメータ値を手動で変更する必要が生じる場合があります。デフォルト値を復元するには **RunAppList** = AGENT (または空のまま)、**UseEnterpriseMode** = No、**ServerHost** = 127.0.0.1、**ServerPort** = 2193 を指定します。

モニター を無効にするには、/etc/drweb/drweb-monitor ファイル内の **ENABLE** 変数の値を 1 から 0 に変更します。

コマンドラインパラメータ

Doctor Web Scanner、SpIDer Guard 及び **Control Center** コンポーネントは、多くのコマンドラインパラメータをサポートしています。これらは、空白とハイフン«-»で指定したパスから分離されます。パラメータの完全なリストを確認するには、 -h 、もしくは --help パラメータを付与して対応するコンポーネント (drweb, drweb-spider or drweb-cc) を起動してください。

Doctor Web Antivirus for Linux パラメータ

Dr.Web Antivirus for Linux の全てのパラメーター覧を見るには、drweb-cc コンポーネントを -h または --help パラメータで開始してください。

Parameter	Description
-a, --agent = <path>	エージェントのパスを指定します ("local:" もしくは "unix:" プリフィックスを使用)
-e, --es	集中管理モードを有効にします。
-c, --conf = <file>	コンフィグレーションファイルのパスを指定します。
-d, --debug = <Errors | Alerts | Info | Verbose | Debug>	ログの詳細レベルを設定（可能な値：Errors、Alerts、Info、Verbose、Debug）。
-v, --version	コンポーネントのバージョン番号を出力。
-s, --scan <path1 path2>	パスが指定されている場合、該当するディレクトリが検査されます。指定されてない場合は、 スケジュール 内で指定したディレクトリが検査されます。**スケジューラ** が無効になっている、またはどのディレクトリも選択されていない場合、スキャナは起動後すぐに終了します（検査するオブジェクトが無いため）。
-g, --guard	**Dr.Web SpIDer Guard** を起動。
-t, --tray	トレイに入れる。

Parameter	Description
-f, --fork	バックグラウンドで動作。
-h, --help	ヘルプを表示。

SpIDer Guard パラメータ

SpIDer Guard の全てのパラメーター一覧を見るには、`drweb-spider` コンポーネントを `-h` または `--help` パラメータで開始してください。

パラメータ	説明
-c, --conf = <*path to file*>{*path to file*}	設定ファイルへのパスを指定。
-r, --restart	**SpIDer Guard** が動作している場合、再起動します。
-s, --stdout	デーモンモードを開始せず、ログを引き続き stdout に出力する。
-d, --debug = `{level}`	ログの詳細レベルを設定する。可能な値は[0...10]で、 0 - quiet、2 - error、4 - alert、6 - info、8 - verbose、10 - debug です。
-i, --idle	**SpIDer Guard** はファイルを検査しません。
-v, --version	コンポーネントのバージョン番号を出力。
-h, --help	ヘルプを表示。

スキャナパラメータ

コマンドラインパラメータは空白で区切られ、ハイフン("-")で始まります。全てのパラメータを見るには、コンソールスキャナ を **-?**、**-h** または **-help** パラメータで開始してください。

コンソールスキャナ パラメータには以下の種類があります。

- 検査場所 パラメータ
- 検査対象 パラメータ
- アクション パラメータ
- インターフェース パラメータ

検査エリアパラメータ

ウイルス検査を実行する場所を指定します。

パラメータ	説明
<path> or *[disk://]<path to device file>*	ウイルス検査を実行するパスを指定します。複数のパスを指定することが可能です。. スタートアップパラメータのオプションパスに下記のように指定されていた場合、必要に応じて適切なデバイスのブートセクターを検査し、修復します。 `disk://<path to device file>`
-@[+]<*file*>	指定したファイルに記載されたオブジェクトを検査します。検査終了後にリストファイルを削除したくない場合、プラス記号 "+" を付けます。リストファイルには、定期的に検査するディレクトリへのパス、または1度だけ検査を実行するファイルのリストを含むことが出来ます。
--	検査するオブジェクトのリストを標準入力 (STDIN) から読み込みます。
-sd	サブフォルダ内のファイルを再帰的に検査します。
-fl	シンボリックリンク先のファイルおよびフォルダを検査します。ループするリンクは無視されます。
-mask	ファイル名のマスクを無視します。

検査対象パラメータ

ウイルス検査の対象となるオブジェクトの種類を指定します。

パラメータ	説明
-al	ファイルの拡張子および構造に関わらず、検査パスで指定

パラメータ	説明
	された全てのオブジェクトを検査します。検査パスは **-path** パラメータ内で指定します。 このパラメータは **-ex** パラメータと逆の作用を持ちます。
-ex	設定ファイルの **FilesTypes** パラメータで指定されている拡張子のファイルを検査します。設定ファイルは **-ini** パラメータで指定します。デフォルトでは、以下のファイル拡張子を持つオブジェクトが検査されます。 EXE、COM、DLL、SYS、VXD、OV?、BAT、BIN、DRV、PRG、BOO、SCR、CMD、386、FON、DO?、XL?、WIZ、RTF、CL*、HT*、VB*、JS*、INF、PP?、OBJ、LIB、PIF、HLP、MD?、INI、MBR、IMG、CSC、CPL、MBP、SH、SHB、SHS、SHT*、CHM、REG、XML、PRC、ASP、LSP、MSO、OBD、THE*、NWS、SWF、MPP、OCX、VS*、DVB、CPY、BMP、RPM、ISO、DEB、AR?、ZIP、R??、GZ、Z、TGZ、TAR、TAZ、CAB、LHA、LZH、BZ2、MSG、EML、7Z、CPIO 検査パスは **-path** パラメータ内で指定します。 このパラメータは **-al** パラメータと逆の作用を持ちます。
-ar[**d**|**m**|**r**][**n**]	*.tar 、または圧縮された*.tar.bz2、 *.tbz形式両方のアーカイブファイルを検査します（ARJ、CAB、GZIP、RAR、TAR、ZIPなど）。 パラメータに**d**、 **m**r、**r** 修飾子を追加しない場合、コンソールスキャナ はアーカイブ内で検出された悪意のある、または疑わしいファイルについての報告のみを行います。修飾子が追加された場合は、該当するアクションが実行されます。
-cn[**d**|**m**|**r**][**n**]	コンテナ内のファイルを検査します（HTML、RTF、PowerPointなど）。 パラメータに**d**、 **m**r、**r** 修飾子を追加しない場合、コンソールスキャナ はコンテナ内で検出された悪意のある、または疑わしいファイルについての報告のみを行います。修飾子が追加された場合は、該当するアクションが実行されます。
-ml[**d**|**m**|**r**][**n**]	メールファイルを検査します。 パラメータに**d**、 **m**r、**r** 修飾子を追加しない場合、コンソールスキャナ はメールファイル内で検出された悪意のある、または疑わしいファイルについての報告のみを行います。修飾子が追加された場合は、該当するアクションが実行されます。
-upn	LZEXE、DIET、PKLITE、EXEPACK で圧縮された実行ファイルを検査します。
-ha	未知の脅威を検出するためのヒューリスティック解析を有効

パラメータ	説明
	にします。

いくつかのパラメータには、以下の修飾子を追加することが出来ます。

- **d** ーオブジェクトを削除
- **m** ーオブジェクトを 隔離 に移動
- **r** ーオブジェクトの名前を変更（ファイル拡張子の最初の文字を '#'に置き換えます）
- **n** ーアーカイブ、コンテナ、メールファイル、パッカーの種類の出力を無効にする

アクションに関する詳細は 検出手法とアクション を参照してください。

アーカイブ、コンテナ、圧縮ファイル、メールファイルなどの複合オブジェクト内で悪意のあるオブジェクトが検出された場合、アクションは複合オブジェクト全体に適用されます。

アクションパラメータ

感染した（または疑わしい）オブジェクトに対して適用するアクションを指定します。

パラメータ	説明
-cu[**d**|**m**|**r**]	感染したファイルまたはブートセクターに対して適用するアクションを指定します。修飾子が追加されていない場合、コンソールスキャナ は感染したオブジェクトを修復し、修復不可能なファイルは削除します（**-ic** パラメータ内で他のアクションが指定されていない限り）。修飾子が追加されている場合は該当するアクションが適用され、修復不可能なファイルに対しては **-ic** パラメータ内で指定されたアクションが適用されます。
-ic[**d**|**m**|**r**]	修復不可能なファイルに対して適用するアクションを指定します。修飾子を追加しなかった場合、コンソールスキャナ は脅威についての報告のみを行います。
-sp[**d**|**m**|**r**]	疑わしいファイルに対して適用するアクションを指定します。修飾子を追加しなかった場合、コンソールスキャナ は脅威についての報告のみを行います。
-adw[**d**|**m**|**r**|**i**]	アドウェアに対して適用するアクションを指定します。修飾子を追加しなかった場合、コンソールスキャナ は脅威についての報告のみを行います。
-dls[**d**|**m**|**r**|**i**]	ダイアラーに対して適用するアクションを指定します。修飾子を追加しなかった場合、コンソールスキャナ は脅威についての報告のみを行います。
-jok[**d**|**m**|**r**|**i**]	ジョークプログラムに対して適用するアクションを指定します。修飾子を追加しなかった場合、コンソールスキャナ は脅威についての報告のみを行います。
-rsk[**d**|**m**|**r**|**i**]	潜在的に危険なプログラムに対して適用するアクションを指定します。修飾子を追加しなかった場合、コンソールスキャナ は脅威についての報告のみを行います。
-hck[**d**|**m**|**r**|**i**]	侵入用ツールに対して適用するアクションを指定します。修飾子を追加しなかった場合、コンソールスキャナ は脅威についての報告のみを行います。

パラメータ	説明
いくつかのパラメータには、以下の修飾子を追加することが出来ます。 • **d** ーオブジェクトを削除 • **m** ーオブジェクトを 隔離 に移動 • **r** ーオブジェクトの名前を変更（ファイル拡張子の最初の文字を '#'に置き換えます） • **i** ー脅威を無視（アドウェアなどの小さい脅威に対してのみ使用可能） アクションに関する詳細は 検出手法とアクション を参照してください。 アーカイブ、コンテナ、圧縮ファイル、メールファイルなどの複合オブジェクト内で悪意のあるオブジェクトが検出された場合、アクションは複合オブジェクト全体に適用されます。	

インターフェースパラメータ

コンソールスキャナ の出力を設定します。

パラメータ	説明
-v, -version, --version	製品およびスキャンエンジンのバージョンに関する情報を出力します。
-ki	ライセンスキーとその所有者に関する情報を表示します（UTF8のみ）。
-go	コンソールスキャナ をバッチモードで動作させます。ユーザ入力が必要なプロンプトをスキップし、デフォルト設定で検査が進みます。このモードはファイルの自動検査、例えばハードディスクの毎日、または毎週の検査の際に便利です。
-ot	標準出力（STDOUT）を使用します。
-oq	情報の出力を無効にします。
-ok	全ての検査されたオブジェクトのリストを表示し、感染していないものに **Ok** を付けます。
-log=[**+**] *<path to file>*	指定されたファイルに コンソールスキャナ の動作に関するログを作成します。ファイル名は必須です。ファイルを上書きせずにログを追加したい場合はプラス記号 '+' を追加します。
-ini=*<path to file>*	指定された設定ファイルを使用します。デフォルトでは コンソールスキャナ に設定ファイルはありません。

パラメータ	説明
-lng=*<path to file>*	指定された言語ファイルを使用します。デフォルトの言語は英語です。
-ni	スキャンオプションの設定に設定ファイルを使用しません。コンソールスキャナ　はコマンドラインのパラメータによってのみ設定されます。
ns	中断シグナル（SIGINT）の使用を含む、検査プロセスの中断を無効にします。
--only-key	キーファイルは、起動時にControl　Agentから受信されていません。

ハイフン «-» を使用して、以下のパラメータを無効にすることができます。

```
-ar -cu -ha -ic -fl -ml -ok -sd -sp
```

たとえば、**Scanner** を次のようにコマンドラインから起動します。

```
$ drweb -path <path> -ha-
```

ヒューリスティック解析（デフォルトでは有効）を無効になります。

`-cu`, `-ic` および `-sp` パラメータは、修飾子で指定した任意のアクションを無効にする否定的フォームで、 これらのパラメータの否定的フォームは脅威や疑わしいファイルが検出された場合に通知を行うよう指定しますが、脅威を回避するアクションを行いません。

`-al` および `-ex` パラメータは、否定的フォームを持ちませんが、お互いをキャンセルします。

デフォルトでは（**Scanner** の設定がカスタマイズされておらず、パラメータが指定されていない）、**Scanner** は次のパラメータを伴い起動します。

```
-ar -ha -fl- -ml -sd
```

デフォルトの **Scanner** パラメータ（圧縮、パックされたファイル、及びメールボックスの検査、再帰的検査、ヒューリスティック検査等を含む）は、一般的なケースや日常の検査でご利用いただけるようになっています。 また、ハイフン «-» を使用してパラメータを無効にすることもできます。

電子メールの添付ファイルとして　ウイルスは圧縮ファイル（特に自己解凍形式）として配布されるため、圧縮ファイルやパックされたファイルのスキャンを無効にすること

は、アンチウイルス保護レベルを著しく低下させます。同様に、マクロウイルス(Word、Excel)の感染を受ける可能性のあるオフィスドキュメントは、アーカイブやコンテナ内の電子メールを介して配送されます。

Scanner をデフォルトのパラメータで起動した場合、発見された脅威や疑わしいファイルに対して修復や、いずれのアクションも行いません。これらのアクションを行うには、対応するコマンドラインパラメーターを指定する必要があります。

アクションのパラメータは、状況によって異なる場合があります。推奨は以下の通りです。

- `cu` – 感染したファイルを移動、削除、リネームを行わず、感染したファイル、およびシステムエリアを修復する。
- `icd` – 修復できないファイルを削除する。
- `spm` – 疑わしいファイルを隔離する。
- `spr` – 疑わしいファイルをリネームする。

Scanner が修復アクションを設定して起動した場合、感染したオブジェクトを元の正常な状態に修復を試みます。ただし、この動作は既知のウイルスを検出した場合にのみ可能であり、修復方法はウイルスデータベースに従います。ただし、感染したファイルがウイルスにより著しく損傷していた場合、修復に失敗する可能性もあります。

圧縮ファイルの中に感染したファイルが検出された場合、修復、削除、移動、リネームはできません。このような場合、手動で圧縮ファイルを解凍し、解凍されたファイルを**Scanner** で直接検査してください。

Scanner が**削除**アクションを伴い起動した場合、検出したすべての感染したファイルをディスクから削除します。このオプションは、修復できない(ウイルスによって破損した)ファイルの対処に適しています。

名前の変更 アクションは、**Scanner** は感染したファイル名を指定した拡張子にリネームします(デフォルトでは«`*.#??`»。この場合、拡張子の一文字目は«`#`»となります)。この拡張子は、他のOS(DOS/Windows)がヒューリスティックに疑わしいファイルを検出するのに役立ちます。拡張子を変更することで、これらのOSが、実行形式のファイルを誤って起動したり、ウイルス感染の増大を防ぐことができます。

移動 アクションを有効にした **Scanner** は、感染した、もしくは疑わしいファイルを隔離ディレクトリに移動します。

付録

付録 A. コンピューター脅威の種類

本マニュアルでは、コンピューターやネットワークに対して潜在的または直接的な損害を与え、ユーザの情報や権限を漏洩させるあらゆる種類のソフトウェアを「脅威」と定義します（悪意のあるソフトウェアやその他の望まないソフトウェア）。広義では、コンピューターまたはネットワークのセキュリティに対するあらゆる種類の潜在的な危険を指して「脅威」とする場合があります（ハッカー攻撃に繋がる脆弱性）。

以下に記載する全ての種類のプログラムは、ユーザのデータまたは機密情報を危険にさらすものです。姿を隠さないプログラム（スパム配信ソフトウェアや様々なトラフィックアナライザなど）は、状況によっては脅威と化す可能性はありますが、通常はコンピューター脅威とみなされません。

Doctor Web の分類では、全ての脅威はその危険度に応じて2つの種類に分けられます。

- **危険度の高い脅威** – システム内で破壊的および違法な行為（重要データを削除する、または盗む、ネットワークをクラッシュさせるなど）を実行する、古くからある典型的なコンピューター脅威。この種類のコンピューター脅威には、マルウェアと呼ばれるソフトウェア、つまりウイルス、ワーム、トロイの木馬が含まれます。
- **危険度の低い脅威** – 上記の脅威に比べて危険度の低いコンピューター脅威ですが、悪意のある動作を実行する為に第三者によって利用される場合があります。また、この脅威がシステム内に存在するということは、保護レベルが低いという事を示します。ITセキュリティスペシャリスト達の間では、この脅威はグレイウェアまたはPUP（potentially unwanted programs：不審プログラム）と呼ばれることがあり、アドウェア、ダイアラー、ジョークプログラム、リスクウェア、侵入用ツールが含まれます。

危険度の高い脅威

コンピューターウイルス

この種類のコンピューター脅威は、他のオブジェクト内にそのコードを埋め込む（これを感染と呼びます）ことが出来るという特徴を持っています。多くの場合、感染したファイルはそれ自体がウイルスのキャリアとなり、また埋め込まれたコードは必ずしもオリジナルのものと一致するとは限りません。ほとんどのウイルスは、システム内のデータを破損させる、または破壊する目的を持っています。

Doctor Web の分類では、ウイルスは感染させるオブジェクトの種類に応じて分けられます。

- **ファイルウイルス**－OSのファイル（通常、実行ファイルおよびダイナミックライブラリ）を感染させ、そのファイルの起動と同時にアクティブになります。
- **マクロウイルス**－Microsoft® Officeのドキュメント、およびマクロコマンド（通常、Visual Basicで記述されている）に対応しているその他のアプリケーションを感染させるウイルスです。マクロコマンドは、完全なプログラミング言語で書かれた埋め込み型のプログラムで、例えばMicrosoft® Wordでは、ドキュメントを開く（または閉じる、保存するなど）と自動的にマクロが開始されます。
- **スクリプトウイルス**－スクリプト言語を使用して作成され、他のスクリプト（OSのサービスファイルなど）を感染させます。また、スクリプトの実行が可能な他のファイルフォーマットも感染させることが出来、Webアプリケーションにおけるスクリプティングの脆弱性を悪用します。
- **ブートウイルス**－ディスクのブートレコード、ハードディスクドライブのパーティションまたはマスターブートレコードを感染させます。メモリをほとんど消費せず、システムがロールアウト、再起動、またはシャットダウンするまで、そのタスクを続行出来る状態を保ちます。

多くのウイルスは検出に対抗する何らかの手段を持ち、その手法は常時改良され続けています。全てのウイルスは、その使用する手法に応じて分類することが出来ます。

- **暗号化ウイルス**－ファイル、ブートセクター、またはメモリ内で検出されるのを防ぐため、感染の度に自身のコードを暗号化します。このウイルスのコピーは全て、ウイルス署名として使用される共通のコードフラグメント（復号化プロシージャ）のみを含んでいます。
- **ポリモーフィック型ウイルス**－同様に自身のコードを暗号化しますが、各コピーごとに異なる特別な復号化プロシージャの生成も行います。つまり、この種類のウイルスはシグネチャバイトを持ちません。
- **ステルスウイルス**－その活動を偽り、感染したオブジェクト内に潜むための動作を実行します。この種類のウイルスは、感染させる前のオブジェクトの情報を「ダミー」として表示させ、改変したファイルが検出されないようにします。

ウイルスは、書かれているプログラミング言語（ほとんどの場合アセンブラ、高級プログラミング言語、スクリプト言語など）、または感染させるOSに応じて分類することも出来ます。

コンピューターワーム

ワームは、ウイルスやその他のコンピューター脅威よりも多く見られるようになってきています。ウイルス同様、自身を複製し拡散することが出来ますが、他のプログラムやファイルを感染させません（つまり、拡散する為にホストファイルを必要としません）。ネットワークを通じて（通常、メールの添付ファイル経由で）侵入し、ネットワーク内にある他のコンピューターにコピーを拡散します。ユーザのアクションに応じて、または攻撃するコンピューターを選択する自動モードで拡散を開始します。

ワームは1つのファイル（ワームのボディ）から成っているとは限りません。多くのワームが、メインメモリ（RAM）内にロードした後ワームのボディを実行ファイルとしてネットワーク経由でダウンロードするシェルコードを持っています。シェルコードがシステム内に存在するだけであれば、システムを再起動することで（RAMが削除されリセットされます）ワームを削除することが出来ますが、ワームのボディがコンピューターに侵入してしまった場合はアンチウイルスプログラムのみが対処可能です。

ワームはその拡散速度によって、例えペイロードを持っていない（直接的な被害を与えない）場合でも、ネットワーク全体の機能を破壊する能力を持っています。

Doctor Web の分類では、ワームはその拡散方法によって以下のように分けられます。

- ネットワーム－様々なネットワークおよびファイル共有プロトコル経由で自身のコピーを拡散します。
- メールワーム－メールプロトコル（POP3、SMTPなど）を使用して拡散します。
- チャットワーム－広く使用されているメッセンジャーおよびチャットプログラム（ICQ、IM、IRCなど）のプロトコルを使用します。

トロイの木馬プログラム

この種類のコンピューター脅威は自身を複製せず、他のプログラムを感染させません。トロイの木馬は頻繁に使用されるプログラムに成り代わり、その機能を実行し

ます（または動作を模倣します）。同時に、システム内で悪意のある動作（データを破損または破壊、機密情報を送信など）を実行したり、ハッカーが許可無しにコンピューターにアクセス（例えば第三者のコンピューターに損害を与えるために）することを可能にします。

トロイの木馬の悪意のある特徴はウイルスのものと類似しており、またトロイの木馬がウイルスのコンポーネントであるという場合もあります。しかし、ほとんどのトロイの木馬は、ユーザまたはシステムタスクによって起動される別の実行ファイルとして配布されます（ファイル交換サーバ、リムーバブルストレージ、メール添付ファイルなどを介して）。

トロイの木馬はしばしばウイルスやワームによって配布されることや、他の種類の脅威によっても実行されうる悪意のある動作の多くがトロイの木馬にも起因することから、その分類が難しくなっています。以下のトロイの木馬は、 **Doctor Web** では別の種類として分類されています。

- **バックドア**－既存のアセスおよびセキュリティシステムをすり抜けて侵入者がシステム内にログイン、または権限を必要とする機能を使用することを可能にしてしまうトロイの木馬です。バックドアはファイルを感染させませんが、自身をレジストリ内に書き込んでレジストリキーを改変します。
- **ルートキット**－その存在を隠す目的で、OSのシステム機能を妨害するように設計された悪意のあるプログラムです。さらに、他のプログラム（他の脅威など）のプロセスや異なるレジストリキー、フォルダ、ファイルを隠ぺいすることも出来ます。ルートキットは独立したプログラムとして、または他の悪意のあるプログラムに含まれるコンポーネントとして拡散します。また、その動作モードによって2つのグループに分けられます。ユーザモードで動作するユーザモードルートキット（UMR）と、カーネルモードで動作するカーネルモードルートッキット（KMR）です。UMRはユーザモードライブラリ機能を妨害し、一方、KMRはシステムのカーネルレベルで機能を妨害し、自身の検出を困難にします。
- **キーロガー**－ユーザがキーボードで入力した情報を記録します。その目的は個人情報（ネットワークパスワード、ログイン、クレジットカードデータなど）を盗むことです。
- **クリッカー**－Webサイトのトラフィックを増加させる目的で、またはDDoS攻撃を実行する為にハイパーリンクを別のアドレスにリダレクトします。
- **プロキシ型トロイの木馬**－被害者のコンピューターを介して匿名でインターネットにアクセスします。

トロイの木馬は、Webブラウザのスタートページを変更したり特定のファイルを削除するなど、上記以外の悪意のある動作も実行することがあります。ただしそのような動作もまた、他の種類の脅威（ウイルスやワーム）によって実行される場合がありま

す。

危険度の低い脅威

侵入用ツール

侵入用ツールは、侵入者によるハッキングを可能にするプログラムです。最も一般的なものは、ファイヤーウォールまたはその他のコンピューター保護システムコンポーネントの脆弱性を検出するポートスキャナです。それらのツールはハッカーだけではなく、管理者がネットワークのセキュリティを検査するためにも用いられます。ハッキングに使用することの出来る一般的なソフトウェアや、ソーシャルエンジニアリングテクニックを使用する様々なプログラムも侵入用ツールに含まれることがあります。

アドウェア

通常、ユーザの画面に強制的に広告を表示させるフリーウェアプログラム内に組み込まれたプログラムコードを指します。ただしそのようなコードは、他の悪意のあるプログラム経由で配布されてWebブラウザ上に広告を表示させる場合もあります。アドウェアプログラムの多くは、スパイウェアによって収集されたデータを用いています。

ジョークプログラム

アドウェア同様、この種類の脅威はシステムに対して直接的な被害を与えることはありません。ジョークプログラムは通常、実際には起こっていないエラーに関するメッセージを表示させ、データの損失につながるアクションの実行を要求します。その目的はユーザを驚かせ不快感を与えることにあります。

ダイアラー

広範囲に渡る電話番号をスキャンし、モデムとして応答するものを見つける為の特別なコンピュータープログラムです。その後、攻撃者がその番号を使用することによって被害者に通話料の請求書が送られます。または被害者が気づかぬうちに、モデム経由で高額な電話サービスに接続されます。

リスクウェア

このプログラムはコンピューター脅威として作成されたものではありませんが、システムセキュリティを無効にする可能性のある機能を持っているため、危険度の低い脅威として分類されます。リスクウェアプログラムはデータを破損または削除してしまう可能性があるのみならず、クラッカーや悪意のあるプログラムによってシステムに被

害を与える為に使用されることがあります。そのようなプログラムの中には、様々なリモートチャットおよび管理ツール、FTPサーバなどがあります。

疑わしいオブジェクト

ヒューリスティックアナライザーによって検出される、潜在的なコンピューター脅威があります。そのようなオブジェクトはいかなる脅威（未知のものを含む）でもあり得、また誤検出の場合には安全なオブジェクトである可能性もあります。

疑わしいオブジェクトは解析の為に **Dr.Web** ウイルスラボ に送信してください。

付録 B. 検出手法とアクション

コンピューター脅威の検出および回避には多くの手法があります。**Dr.Web** 製品 はそれらの手法を組み合わせ、柔軟且つユーザフレンドリーな設定、および確かなセキュリティを保証する包括的なアプローチによってコンピューターやネットワークに対する最も信頼性の高い保護を提供します。

検出手法

署名のチェックサム検査

この手法は署名解析の一種で、署名とは、それぞれのコンピューター脅威が持つユニークな一連の有限バイトシーケンスです。ウイルスデータベースに存在する署名が、検査されたプログラムコード内で見つかった場合、検出へとつながります。

署名のチェックサム検査は、署名そのものではなく署名のチェックサムを比較します。それによりウイルスデータベースのサイズを大幅に減らし、従来の署名解析の信頼性を維持します。

実行のエミュレーション

プログラムコード実行のエミュレーション手法は、署名のチェックサム解析が効果的ではない場合、または著しく困難な場合（サンプルから信頼できる署名を抽出できないため）に、ポリモーフィックや暗号化ウイルスを検出するために使用されます。CPUのソフトウェアモデルであるエミュレータが、解析されたサンプルコードの実行をエミュレートします。指令は保護されたメモリスペース（エミュレーションバッファ）内で

実行され、CPUに渡されて実際に実行されることはありません。感染したファイルがエミュレータによって処理されると、ウイルスのボディが復号化され、署名のチェックサム解析によって簡単に定義されるようになります。

ヒューリスティック解析

ヒューリスティック解析は、ウイルスデータベースにそのバイト署名が追加されていない、新たに作成された未知の脅威を検出する為に使用され、コンピューター脅威に典型的な、または滅多に見られない特徴の重みの定義または計算に基づいて行われます。それらの特徴はその重み（特徴の重要さを定義する数値）およびサイン（ポジティブなサインはその特徴がコンピューター脅威に典型的なものであることを示し、ネガティブなサインは脅威とは関連の無い特徴であることを示します）を持っています。オブジェクトにおけるそれらの合計が特定の閾値を超えている場合、ヒューリスティックアナライザによって脅威である可能性があると判定され、疑わしいオブジェクトと定義されます。

その他の仮説に基づいた検査システム同様、ヒューリスティック解析は誤検出（タイプIエラー）および見逃し（タイプIIエラー）の可能性があります。

Origins Tracing™

Origins Tracing™ は **Doctor Web** によって開発され **Dr.Web 製品** でのみ使用されている、ユニークな非署名脅威検出アルゴリズムです。従来の署名ベースの検査およびヒューリスティック解析と合わせて、未知の脅威の検出を大幅に向上させます。**Origins Tracing** アルゴリズムを使用して検出されたオブジェクトの名前には.Origin拡張子が付きます。

アクション

コンピューター脅威を回避する為に、**Dr.Web 製品** は悪意のあるオブジェクトに対して様々なアクションを適用します。ユーザはデフォルト設定を使用、自動的に適用するアクションを設定、または検出の度に手動でアクションを選択することが出来ます。使用可能なアクションは以下のとおりです。

* **修復**－危険度の高い脅威（ウイルス、ワーム、トロイの木馬）に対してのみ適用可能なアクションです。感染したオブジェクトから悪意のあるコードを削除し、可能であれば、オブジェクトの感染前の構造および動作を復元します。 悪意のあるオブジェクトは悪意のあるコードのみで構成されている場合があり（トロイの木馬やコンピューターワームのコピーなど）、その場合、システムの修復はオブジェクト全体の完全な削除を意味します。ウイルスに感染したファイルが全て修復可能なわけではありませんが、修復アルゴリズム

は常に改良され続けています。

- **隔離**（隔離に移動）－検出された脅威を特別なフォルダに移し、残りのシステムから隔離します。このアクションは修復が不可能な場合、また全ての疑わしいオブジェクトに適しています。そのようなファイルのコピーは解析の為 **Dr.Web ウイルスラボ** に送信することを推奨します。
- **削除**－コンピューター脅威を回避する最も効果的なアクションで、あらゆる種類のコンピューター脅威に対して適用可能です。このアクションは、修復アクションが選択されているオブジェクトに対して適用されることがあり、これはオブジェクトが悪意のあるコードのみで構成され有益な情報を持っていない場合（例えば、コンピューターワームの修復が、そのコピーを全て削除することを意味する場合など）に起こります。
- **名前の変更**－感染したファイルの拡張子を、指定されたマスクに応じて変更します（デフォルトでは、拡張子の最初の記号が # に置き換えられます）。 このアクションは、ヒューリスティックによって疑わしいと判定された、他のOS（MS-DOS®、Microsoft® Windows®など）のファイルに適しています。名前の変更によって、それらのOS内にある実行ファイルを誤って起動することを回避し、ウイルス感染やその拡大を防ぎます。
- **無視**－危険度の低い脅威（アドウェア、ダイアラー、ジョークプログラム、侵入用ツール、リスクウェア）に対してのみ適用可能なアクションで、いずれのアクションも実行せず通知も表示せずに脅威をスキップします。
- **レポート**－アクションは適用されず、脅威は結果のレポートに記載されます。

付録 C. サポート

Dr.Web 製品の有償版を購入されたカスタマーはサポートサービスをご利用いただけます。http://support.drweb.co.jp/ の **Doctor Web テクニカルサポート** をご覧ください。

製品のインストールまたは使用に関する問題が発生した場合、以下の **Doctor Web** サポートオプションをご利用ください。

- http://download.drweb.co.jp/ から最新のマニュアルおよびガイドをダウンロードして見る
- http://support.drweb.co.jp/ で、よくある質問を見る
- http://wiki.drweb.com/ で、Dr.Web knowledge databaseの回答を確認する

- http://forum.drweb.com/ で、Dr.Webオフィシャルフォーラムを閲覧する

問題が解決しなかった場合、サポートサイト http://support.drweb.co.jp/ の該当するセクションでwebフォームに入力し、直接 **Doctor Web テクニカルサポート** にお問い合わせください。

会社情報は、 **Doctor Web オフィシャルウェブサイト** http://company.drweb.com/contacts/moscow を参照して下さい。

付録 D. 集中管理

Doctor Web の集中管理は、論理構造内にあるコンピューター（例えば、企業ローカルネットワーク内外からお互いにアクセスする企業のコンピューターなど）の情報セキュリティの設定および管理を自動化・簡易化します。保護されるコンピューターは、管理者が集中管理サーバからそのセキュリティを監視および管理するアンチウイルスネットワーク内で1つに統合されます。集中管理されているアンチウイルスシステムへの接続によって、エンドユーザによる操作を最小限に抑えると同時にレベルの高い保護を保証します。

アンチウイルスネットワークの論理構造

Doctor Web の集中管理はクライアントサーバモデルを使用します（下図参照）。

ワークステーションとサーバはインストールされた *ローカルアンチウイルスコンポーネント*（エージェントまたはクライアント、本マニュアルでは **Dr.Web Anti-virus for Linux** ）によって保護され、それによってリモートコンピューターに対するアンチウイルス保護を提供し、集中管理サーバ への容易な接続を確かなものにします。

ローカルコンピューターのアップデートおよび設定は *集中管理サーバ* から行われます。アンチウイルスネットワーク内の指令、データおよび統計情報もまた集中管理サーバを経由します。保護するコンピューターと中央サーバ間のトラフィックは非常に大きくなる可能性があるため、圧縮のオプションを使用することが出来ます。機密情報の漏洩やダウンロードしたソフトウェアのすり替えを回避する為、暗号化にも対応しています。

必要な全てのアップデートは **Dr.Web Global Update System** サーバから集中管理サーバにダウンロードされます。

ローカルアンチウイルスコンポーネントは、*アンチウイルスネットワーク管理者* からのコマンドに応じて集中管理サーバから設定および管理されます。管理者は集中管理サーバ、およびアンチウイルスネットワークトポロジーを管理し(リモートコンピュータから集中管理サーバへの接続を有効にするなど)、必要な場合はローカルアンチウイルスコンポーネントの動作を設定します。

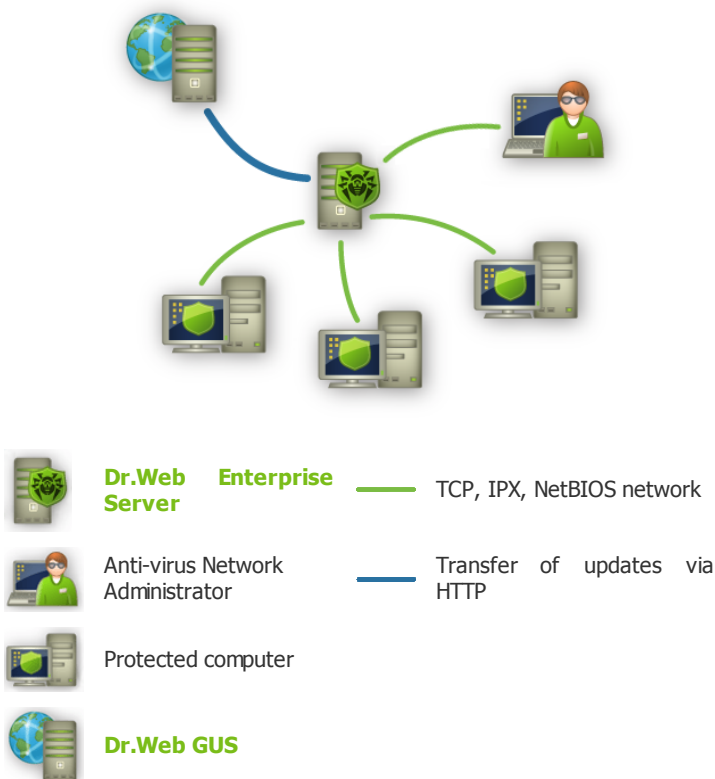



図 32. アンチウイルスネットワークの論理構造

ローカルアンチウイルスコンポーネントは、集中管理モードに対応していない **Dr.Web アンチウイルスソリューション**（例：**Dr.Web® Anti-virus for Linux** バージョン 5.0）を含むその他のアンチウイルスソフトウェアとの互換性を持ちません。同一コンピューター上への2つ以上のアンチウイルスプログラムのインストールは、システムのクラッシュや重要なデータの損失を引き起こす場合があります。